MODELAMIENTO DE LOS PROCESOS DE AUDITORÍA EN SEGURIDAD DE LA INFORMACIÓN ASOCIADOS A LOS DOMINIOS 6, 8, 13 Y 14 DEL ANEXO A DE LA NORMA ISO 27001 MEDIANTE UNA HERRAMIENTA DE FLUJO DE TRABAJO

INFORME FINAL

JUAN MANUEL VELÁSQUEZ ISAZA

4516755

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y DE SISTEMAS Y COMPUTACIÓN
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA

25 de marzo de 2015

MODELAMIENTO DE LOS PROCESOS DE AUDITORÍA EN SEGURIDAD DE LA INFORMACIÓN ASOCIADOS A LOS DOMINIOS 6, 8, 13 Y 14 DEL ANEXO A DE LA NORMA ISO 27001 MEDIANTE UNA HERRAMIENTA DE FLUJO DE TRABAJO

JUAN MANUEL VELÁSQUEZ ISAZA

4516755

Trabajo de Grado para optar el titulo de
INGENIERO DE SISTEMAS Y COMPUTACIÓN

Dirigida por la Magister en Ingeniería
ANA MARÍA LÓPEZ ECHEVERRY

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y DE SISTEMAS Y COMPUTACIÓN
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA

25 de marzo de 2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

25 de marzo de 2015

"Para todos aquellos que han perseverado por alcanzar sus sueños,
para aquellos que nunca se rindieron sin importar la adversidad,
y para quienes han creído que todo es posible,
de ellos es este logro que hoy alcanzo..."

Juan Manuel Velásquez Isaza

Agradecimientos

. . . El camino labrado hasta ahora ha sido producto de la dedicación, perseverancia y sacrificios para sobreponerme a las dificultades y adversidades presentadas en este largo camino hacia la culminación de un peldaño más de tantos que aun debo alcanzar, el cual fue posible lograr gracias al apoyo, comprensión, reclamos, regaños, presiones, tomadas de pelo, exigencias y demás formas de expresión que, de una u otra forma, han sido esa "batería" inagotable de aliento para llegar hasta aquí.

De manera particular, agradezco:

En primera instancia a mis padres, por su incondicional apoyo y compresión, así como de los incontables reproches y reclamos, en los momentos más difíciles de mi vida y a quienes les debo ser la persona que hoy soy...

A mi directora de proyecto de grado Ana María López Echeverry, quien ha depositado una gran confianza y cuya guía ha permitido mi crecimiento profesional y académico, y fruto de ello es el resultado de este proyecto...

Así mismo, agradezco a Paula Andrea Villa, Luz Stella Valencia, Carlos Alberto Ocampo y Hugo Humberto Morales, quienes con sus constantes presiones, consejos y apoyo incondicional, permitieron culminar esta etapa académica...

A mi familia, por ese apoyo moral de tantos años viendo mis trasnochos, ausencias en encuentros familiares y momentos de enojo producto de las dificultadas durante mi carrera, sin contar de los gratos momentos que como familia hemos realizado, hoy dan fe de la culminación de una etapa más en mi vida...

A Magda Luz Londoño Giraldo y familia, por su apoyo y comprensión incondicional, por su presión para culminar pronto esta etapa y por siempre estar allí cuando menos lo esperaba...

A la empresa que permitió realizar la prueba piloto del modelo de auditoría propuesto...

A mis compañeros de trabajo y de **SIAN OPEN HARD**, por todo su apoyo, risas y gratos momentos, quienes han estado allí cuando las cosas parecían desfallecer para animar y buscar juntos una solución a tantas dificultades por las que tanto les debo...

Finalmente, aunque no por eso menos importantes, agradezco a mis amigos, por comprender mis ausencias y permanecer a mi lado en los momentos mas difíciles, quienes con su alegría no permitieron que decayera...

Índice

Índice de figuras

Índice de Tablas

INTRODUCCIÓN

Hace algunos años, lo relevante para toda organización eran las estrategias para hacer rentable su Know-How y resguardarlo de la competencia. Con el tiempo, los avances tecnológicos llegaron y consigo mucho de ese conocimiento quedó obsoleto y rezagado frente a ideas innovadoras y de vanguardia. Hoy en día las empresas giran alrededor de su conocimiento y la manera como hacen uso de la información que ésta genera. Sin embargo, es clara la brecha existente entre la tecnología y la forma como se realiza de manera segura las operaciones al interior de la organización para garantizar la confidencialidad, disponibilidad e integridad de esa información que pasa, en la mayoría de los casos, por manos de uno, dos o más empleados sin tomar las medidas adecuadas para su correcto tratamiento.

El grado de desconocimiento de las empresas en la seguridad de la información es elevado y esto se evidencia con el constante ataque del que han sido víctima por no contar con los mecanismos de protección adecuados, vulnerando no solo su información sino también su buen nombre y prestigio.

Por tal motivo, las empresas deberían apropiarse de las buenas prácticas de seguridad y aplicar alguno de los estándares existentes. El presente informe es el resultado del análisis realizado a la norma **NTC-ISO/IEC 27001:2006** para ser aplicado en el diseño de una arquitectura y de las herramientas necesarias para auditar un sistema de gestión de seguridad de la información por parte de auditores internos en los aspectos *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humano"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"*.

FORMULACIÓN DEL PROBLEMA

Dentro de los resultados que se presentan en "VI Encuesta Latinoamericana de Seguridad de la Información ACIS 2014"[1] , se observa un leve aumento en el uso de buenas prácticas, encontrando un 5 % de aumento de aplicación de la ISO 27001 en relación al año pasado (de 58,33 % en 2013 a 63,33 % en 2014); el mismo comportamiento se aprecia en los demás estándares. El alto porcentaje de situaciones críticas presentadas en las organizaciones son en su mayoría causada por falta de ética, debido a la falta de concientización en temas de seguridad de la información. El informe muestra también la falta de apoyo a la dirección para la implementación de la seguridad de la información decae al 41,85 % para el año 2014, 6,48 % menos que el año anterior. Es notable el crecimiento y desarrollo tecnológico e innovación de los grupos delictivos en la región, lo cual no refleja un crecimiento significativo en el fortalecimiento del área de SI o de buenas prácticas.

Al poner el contexto de la realidad que se presenta en Colombia, la Superintendencia de Industria y Comercio durante el mes de marzo de 2010 a marzo de 2011[2] , ha impuesto 86 multas por infracción a la Ley 1266 de 2008, comúnmente conocida como Ley de habeas data financiero. Todas ellas suman $1.951.026.150. Un dato más reciente presentado por la misma entidad[3] revela que al 22 de marzo de 2013 se han impuesto 544 multas para un total de $ 4.719.129.675 pesos. Con lo anterior se deja claro que las empresas deben adoptar medidas para evitar lesionar los derechos de los titulares de los datos personales. En este panorama se aprecia claramente no solo pérdida de dinero y tiempo, sino también como se ve comprometido el buen nombre, la credibilidad y la confianza ante clientes y terceros se desmoronan.

La problemática planteada deja ver la necesidad de implementar controles adecuados que les permita a los auditores internos velar por el cumplimiento de los estándares en cuanto a seguridad de la información se refiere.

En el proyecto *"Sistema de gestión de seguridad soportado en TIC´s para realizar un aporte a la competitividad de las empresas de la región"*[4] , se plantea un modelo de seguridad de la

[1] VI Encuesta Latinoamericana de Seguridad de la Información ACIS 2014. [En línea] *<http://acis.org.co/fileadmin/Base_de_Conocimiento/XIV_JornadaSeguridad/ELSI_2014.pdf>*. [Citado el 14 de julio de 2014]

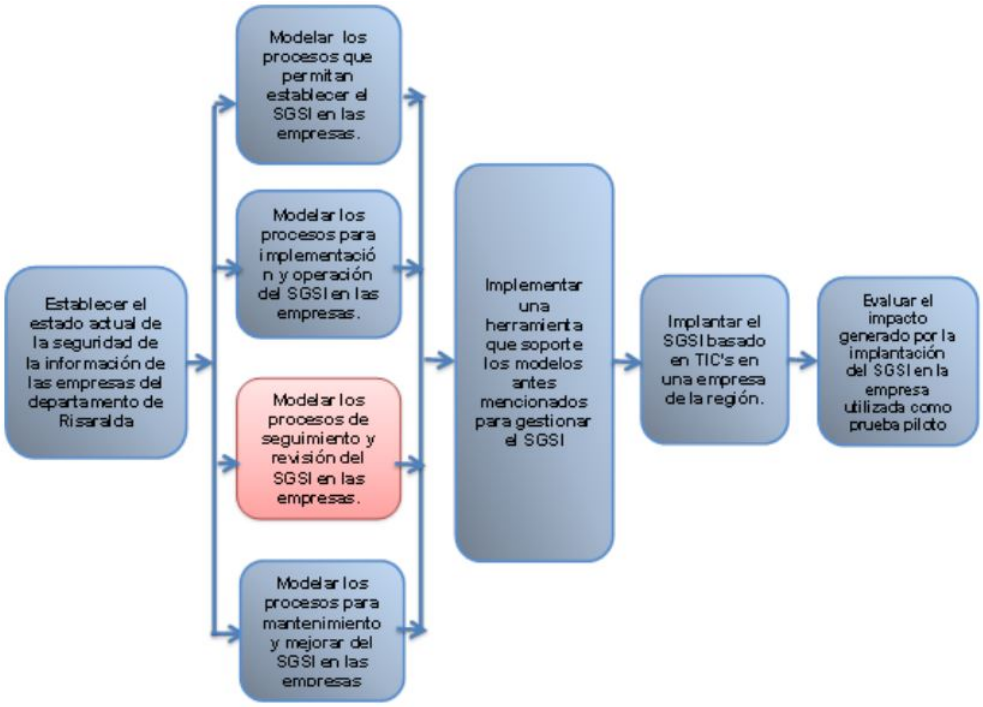
[2] Más de 1900 millones de pesos en multas por infracciones a la ley 1266. [En línea] *<http://habeasdatacolombia.uniandes.edu.co/?p=168>*. [Citado el 5 de julio de 2012]

[3] 41 personas condenadas por el delito de violación de datos personales y 544 multas por infracción de la ley 1266 de 2008, [en línea] *<http://habeasdatacolombia.uniandes.edu.co/?p=980>* [Citado 14 de julio de 2014].

[4] Paula A. Villa S. DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TICś. Universidad Tecnológica de Pe-

información, cuyos módulos se indican en la Figura 2.1. Actualmente, el modelo no cuenta con los aspectos *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"* en su módulo *"Modelar los procesos de seguimiento y revisión del sistema de gestión de seguridad de la información en las empresas"*, los cuales son objeto de estudio de este proyecto de grado.

Figura 2.1: *Módulos del proyecto sistema de gestión de seguridad soportado en TICś para realizar un aporte a la competitividad de las empresas de la región.*



Fuente: Definición de procesos de auditoría interna del sistema de gestión de seguridad de la información soportado en TICś[5]

reira, 2011. Pág.23.

[5]Paula A. Villa S. DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TICŚ. Universidad Tecnológica de Pereira, 2011. Pág.24.

JUSTIFICACIÓN

Se contará con una metodología que permita a los auditores internos en seguridad de la información contar con una herramienta de flujo de trabajo para realizar su proceso de auditoría en las áreas incluidas dentro del alcance considerado por la empresa auditada; además, se podrá validar el impacto generado en una empresa que tiene implementado un Sistema de Gestión de Seguridad de la Información o similar y determinar, mediante una lista de chequeo, el cumplimiento de los dominios 6, 8, 13 y 14 del anexo A de la **NTC-ISO/IEC 27001:2006** al interior de ella.

Dentro de los beneficios que se generan al realizar este proyecto se encuentra:

- Se contará con los conocimientos necesarios para comprender los procesos de una auditoría de un sistema de gestión de seguridad de la información y la aplicación de la norma **NTC-ISO/IEC 27001:2006** en ella.
- Servirá como punto de partida para procesos investigativos orientados al desarrollo de nuevas metodologías que sirvan de apoyo en los procesos de auditoría en seguridad de la información para las empresas de la región.
- Se contará con una herramienta computacional para el control del proceso de auditoría en los aspectos de la norma **NTC-ISO/IEC 27001:2006** referentes a los aspectos: *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"*.

HIPÓTESIS Y OBJETIVOS

4.1. HIPÓTESIS

¿Es posible modelar un proceso de auditoría interna basado en procesos asociado a los dominios 6, 8, 13 y 14 del anexo A de la norma **NTC-ISO/IEC 27001:2006** que sirva de apoyo a los auditores internos para las auditorías en seguridad de información al momento de llevar a cabo una auditoría de seguridad de la información?

4.2. OBJETIVO GENERAL

Modelar los procesos de auditoría interna de un Sistema de Gestión de Seguridad de la Información asociados a los dominios 6, 8, 13 y 14 del Anexo A de la norma **NTC-ISO/IEC 27001:2006**, usando una herramienta orientada a la Web para modelamiento de procesos de negocio.

4.3. OBJETIVOS ESPECÍFICOS

- Modelar los procesos de auditoria correspondientes al domino 6 del anexo A la norma **NTC-ISO/IEC 27001:2006**, *"Organización de la seguridad de la información"*.
- Modelar los procesos de auditoria correspondientes al dominio 8 del anexo A la norma **NTC-ISO/IEC 27001:2006**, *"Seguridad de los recursos humanos"*.
- Modelar los procesos de auditoria correspondientes al dominio 13 del anexo A la norma **NTC-ISO/IEC 27001:2006**, *"Gestión de los incidentes de la seguridad de la información"*.
- Modelar los procesos de auditoria correspondientes al dominio 14 del anexo A la norma **NTC-ISO/IEC 27001:2006**, *"Gestión de la continuidad del negocio"*.
- Verificar el correcto funcionamiento de la implementación de los dominios 6, 8, 13 y 14 del anexo A la norma **NTC-ISO/IEC 27001:2006** mediante una prueba piloto.

MARCO DE REFERENCIA

5.1. MARCO DE ANTECEDENTES

En el artículo *Application of models in information security management*[1] se realiza un modelado de diagramas de clase para una implementación basada en la norma **ISO 27001:2005**. El meta-modelo resultante fue adaptado luego de realizase un análisis semántico. En el trabajo realizado, se apoyaron en otra norma de la familia ISO 27000 (ISO 27005) para el desarrollo de la implementación. Lo interesante se aprecia en el modelo para la detección de amenazas y vulnerabilidades, presente en todo SGSI.

En *Automation possibilities in information security management*[2] se usa un modelo por procesos para el desarrollo de una aplicación para la automatización en la gestión de seguridad de la información. El artículo presenta un esquema con una ontología de seguridad, mostrando los conceptos de alto nivel y las relaciones de la ontología de seguridad, en el que las amenazas, las vulnerabilidades, los controles, y sus implementaciones son los elementos fundamentales. La herramienta **AURUM** utiliza la ontología de seguridad y los motores de razonamiento para calcular los niveles actuales de riesgo de los activos y ofrecer sugerencias de aplicación correspondientes a medidas a tomar para reducir el riesgo a un nivel aceptable. Si el riesgo excede el nivel aceptable, AURUM sugiere automáticamente las implementaciones de los controles adecuados. Finalmente, se explica el *Protocolo de Automatización de Contenido de Seguridad (Security Content Automation Protocol - **SCAP**)*. SCAP puede ser utilizada en la fase de comprobación del proceso de gestión de seguridad de la información a fin de proporcionar una forma automatizada para realizar la supervisión continua de la configuración del sistema de seguridad, examinar los sistemas de signos de compromiso, y para ser capaz de determinar la posición de seguridad de los sistemas y de la organización en cualquier momento dado.

Algunas de las preocupaciones más comunes presentes en la mayoría de las empresas respecto al manejo de la información se muestra en *Information security management - a practical approach*[3] . Presenta los pasos necesarios para el establecimiento y la gestión completa de la seguridad de la información en una organización con normas ya establecidas. Muestra, además, los problemas humanos más comunes en el ámbito de la seguridad de la información. Con esto, se busca concientizar a las organizaciones de las implicaciones en seguridad de la información y llegar a obtener una referencia rápida y oportuna del punto de partida para la solución de sus problemas de seguridad existentes.

[1] Application of models in information security management. Milicevic, Danijel; Goeken, Matthias. IEEE Computer Society, 2011.

[2] Automation possibilities in information security management. Montesino, Raydel; Fenz, Stefan. 2011 European Intelligence and Security Informatics Conference. IEEE Computer Society, 2011.

[3] Information security management - a practical approach. Dey, Manik. IEEE Computer Society, 2010.

En *Privacy and information security in brazil? yes, we have it and we do it!*[4] Se hace una implementación de un SGSI en una empresa del sector público en Brasil. Allí se explican algunos referentes a la seguridad de la información y de la importancia de implementar un SGSI en una organización, en particular en esta empresa brasilera. La importancia de la implementación radica en establecer políticas adicionales para garantizar que los datos y las aplicaciones del sistema cumplan a cabalidad el servicio que presta la comunidad de Sao Paulo. También se destaca la metodología usada para el análisis y evaluación de los riesgos, indispensables para la continuidad del negocio.

Lo anterior deja claro el interés de las organizaciones y de entidades dedicadas a la seguridad de la información de la importancia de contar con un sistema de gestión que permita detectar oportunamente riesgos potenciales en la organización. Sin embargo, en Latinoamérica se continúa notando falencias significativas en cuanto a la seguridad de la información. Pese al incremento por la adopción de buenas prácticas presentado por las empresas, durante la *"VI Encuesta Latinoamericana de Seguridad de la Información ACIS 2014"*[5] , se presenta el estudio con las tendencias que revelan muchas de estas preocupaciones y los patrones de acción para los profesionales en seguridad de la información.

5.2. MARCO TEÓRICO

5.2.1. FAMILIA ISO 9000

La lista de normas de la familia ISO 9000 ha sido elaborada para asistir a las organizaciones, de todo tipo y tamaño, en la implantación y el funcionamiento de sistemas de la calidad efectivos. A continuación se muestra la descripción general de cada una de ellas[6] :

- **ISO 9000:** Ha sido preparada por el Comité Técnico ISO/TC 176. Describe los fundamentos de los sistemas de gestión de la calidad y especifica la terminología de los sistemas de gestión de la calidad.
- **ISO 9001:** Especifica los requisitos para los sistemas de gestión de la calidad aplicables a toda organización que necesite demostrar su capacidad para proporcionar productos

[4]Privacy and information security in brazil? yes, we have it and we do it! Mana G., Joel. 2010 Seventh International Conference on Information Technology. IEEE Computer Society, 2010.

[5]VI Encuesta Latinoamericana de Seguridad de la Información ACIS 2014. [En línea], *http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XIV_JornadaSeguridad/ELSI_2014.pdf.* [Citado el 14 de julio de 2014].

[6]*ISO 9000:* Sistema de gestión de la calidad. Conceptos y vocabulario

que cumplan los requisitos de sus clientes y los reglamentarios que le sean de aplicación y su objetivo es la consecución de la satisfacción del cliente.

- **ISO 9004:** Proporciona directrices que consideran tanto la eficacia como la efectividad del sistema de gestión de la calidad. El objetivo de esta norma es la mejora del desempeño de la organización y la satisfacción de los clientes y de las partes interesadas.
- **ISO 19011:** Proporciona directrices relativas a las auditorías de gestión de la calidad y de gestión medioambiental.

5.2.2. LA SERIE ISO 27000

ISO/IEC 27000[7] es un conjunto de estándares desarrollados - o en fase de desarrollo - por ISO (Internacional Organization for Standardization) e IEC (Internacional Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La 27000 es realmente una serie de estándares, reservando los rangos de numeración de 27000 a 27019 y de 27030 a 27044.

- **ISO/IEC 27000:** Contiene términos y definiciones que se emplean en toda la serie 27000.
- **NTC-ISO/IEC 27001:2006:** Contiene los requisitos del SGSI. Tiene su origen en la BS 77700-2:2000 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la **NTC-ISO/IEC 27002:2007**, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
- **NTC-ISO/IEC 27002:2007:** Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

En octubre de 2013, tanto la ISO 27001 como ISO 27002 sufrieron cambios considerables en su estructura y contenido. Sin embargo, para dar continuidad a los proyectos que ya se había desarrollado bajo el estándar NTC-ISO/IEC 27001:2006 este proyecto se desarrolló usando esta misma versión del estándar y se propone, como un trabajo futuro, ajustar los proyectos anteriores al estándar NTC-ISO/IEC 27001:2013, la cual es la actual versión para Colombia. Sólo se encuentra publicada la ISO/IEC 27002:2013 como estándar internacional; en Colombia se encuentra en proceso de adaptación.

[7] *ISO 27000.* [En línea], *www.iso27000.es*

5.2.3. COBIT

CobiT[8] es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. CobiT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

CobiT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI. El uso de las TI es una inversión importante que debe ser gestionado. CobiT ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y sea probable que entreguen los beneficios esperados.

CobiT permite el desarrollo de políticas claras y mejores prácticas para la administración de TI. El marco ayuda a aumentar el valor obtenido de TI. También ayuda a las organizaciones a gestionar los riesgos relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Debido a que CobiT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. CobiT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Los siguientes son los resultados de la adopción de CobiT:

- Los gerentes y el staff de TI entenderán totalmente como es que el negocio y TI pueden trabajar en forma conjunta para la entrega exitosa de las iniciativas de TI.
- Los costos totales del ciclo de vida de TI serán más transparentes y predecibles.
- TI ofrecerá información más oportuna y de mayor calidad.
- TI entregará proyectos de mejor calidad y más exitosos.
- Los requisitos de seguridad y privacidad serán más claros y la implementación será monitoreada con mayor facilidad.
- Los riesgos de TI serán gestionados con mayor eficacia.
- Las auditorías serán más eficientes y exitosas.

[8] Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa. Un reporte para gestión del ITGI y la OGC. IT GOVERNANCE INSTITUTE. [En línea], *http://www.ISACA.com/*

- El cumplimiento de TI con los requisitos regulatorios serán una práctica normal de gestión.

CobiT se estructura en cuatro partes; la principal de ellas se divide de acuerdo con 34 procesos de TI. Cada proceso se cubre en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso. Utiliza un ciclo de vida de tipo PDCA que lo integra en los procesos de negocio.[9] Para cada uno de ellos se define:[10]

- Definición del proceso.
- Indicadores de información y dominio.
- Objetivos de TI.
- Objetivos del proceso.
- Prácticas claves.
- Métricas.
- Gobierno y recursos de TI.

5.3. MARCO CONCEPTUAL

5.3.1. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

5.3.1.1. Definición

La auditoría de sistemas[11] es la revisión y la evaluación de los controles, sistemas, procedimientos de un sistema de información, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de esa información, a fin de brindar por medio del señalamiento de cursos alternativos lograr una utilización más eficiente y segura de la información y llevar a la dirección a una adecuada toma de decisiones.

[9] Otros estándares. [En línea], *http://www.iso27000.es/otros_estandar.html*
[10] Cobit 5 y la Seguridad de la información. [En línea], *http://www.ISACA.com/*
[11] Auditoría de sistemas. Jorge Alberto Blanco Duarte. Escuela superior de administración pública.

5.3.1.2. Procedimientos de auditoría

El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos.

El proceso de auditoría exige que el auditor de sistemas reúna[12] :

- Evidencia evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada.
- Prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia.

a. Planificación de una auditoria

Una planificación adecuada es el primer paso necesario para realizar auditorías de sistema eficaces. El auditor de sistemas debe comprender el ambiente del negocio en el que se ha de realizar la auditoría así como los riesgos del negocio y control asociado. Las áreas que deben ser cubiertas durante esta etapa son:

- Comprensión del negocio y de su ambiente.
- Riesgo y materialidad de auditoría.
- Técnicas de evaluación de Riesgos.
- Objetivos de controles y objetivos de auditoría.
- Procedimientos de auditoría.

b. Desarrollo del programa de auditoria

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoría planificados. El esquema típico de un programa de auditoría incluye lo siguiente:

- **Tema de auditoría:** Donde se identifica el área a ser auditada.

[12] Metodología de una auditoria de sistemas. Miguel Ángel Durán Jacobo. Instituto Tecnológico de Chetumal. [En línea], *http://www.itchetumal.edu.mx/paginasvar/Maestros/mduran/Archivos/METODOLOGIA %20DE %-20UNA %20AUDITORIA %20DE %20SISTEMAS.pdf*

- **Objetivos de Auditoría:** Donde se indica el propósito del trabajo de auditoría a realizar.
- **Alcances de auditoría:** Aquí se identifica los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.
- **Planificación previa:** Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
- **Procedimientos de auditoría:**
  - Recopilación de datos.
  - Identificación de lista de personas a entrevistar.
  - Identificación y selección del enfoque del trabajo.
  - Identificación y obtención de políticas, normas y directivas.
  - Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
  - Procedimientos para evaluar los resultados de las pruebas y revisiones.
  - Procedimientos de comunicación con la gerencia.
  - Procedimientos de seguimiento.

El programa de auditoría se convierte también en una guía para documentar los diversos pasos de auditoría y para señalar la ubicación del material de evidencia.

c. Asignación de recursos de auditoría

La asignación de recursos para el trabajo de auditoría debe considerar las técnicas de administración de proyectos las cuales tienen los siguientes pasos básicos:

- **Desarrollar un plan detallado:** El plan debe precisar los pasos a seguir para cada tarea y estimar de manera realista, el tiempo teniendo en cuenta el personal disponible.
- **Contrastar la actividad actual con la actividad planificada en el proyecto:** debe existir algún mecanismo que permita comparar el progreso real con lo planificado. Generalmente se utilizan las hojas de control de tiempo.
- **Ajustar el plan y tomar las acciones correctivas:** si al comparar el avance con lo proyectado se determina avances o retrasos, se debe reasignar tareas. El control se puede llevar en un diagrama de Gantt.

Los recursos deben comprender también las habilidades con las que cuenta el grupo de trabajo de auditoría y el entrenamiento y experiencia que estos tengan. Además, tener en cuenta la

disponibilidad del personal para la realización del trabajo de auditoría.

d. Técnicas de recopilación de evidencias.

La recopilación de material de evidencia es un paso clave en el proceso de la auditoría. El auditor de sistemas debe tener conocimiento de cómo puede recopilar la evidencia examinada. Algunas formas son las siguientes:

- Revisión de las estructuras organizacionales de sistemas de información.
- Revisión de documentos que inician el desarrollo del sistema; estos no necesariamente se encontrarán en documentos, si no en medios magnéticos para lo cual el auditor deberá conocer las formas de recopilarlos mediante el uso del computador.
- Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no de acusatoria.
- Observación de operaciones y actuación de empleados.
- Auto documentación, es decir el auditor puede preparar narrativas en base a su observación, flujo gramas, cuestionarios de entrevistas realizados.
- Utilización de técnicas de auditoría asistida por computador CAAT.

e. Evaluación de fortalezas y debilidades de auditoría.

Luego de desarrollar el programa de auditoría y recopilar evidencia de auditoría, el siguiente paso es evaluar la información recopilada con la finalidad de desarrollar una opinión. Para esto generalmente se utiliza una matriz de control con la que se evaluará el nivel de los controles identificados, esta matriz tiene sobre el eje vertical los tipos de errores que pueden presentarse en el área y un eje horizontal los controles conocidos para detectar o corregir los errores, luego se establece un puntaje (puede ser de 1 a 10 ó 0 a 20, la idea es que cuantifique calidad) para cada correspondencia, una vez completada, la matriz muestra las áreas en que los controles no existen o son débiles, obviamente el auditor debe tener el suficiente criterio para juzgar cuando no lo hay si es necesario el control.

En esta parte de evaluación de debilidades y fortalezas también se debe elegir o determinar la materialidad de las observaciones o hallazgos de auditoría. El auditor de sistemas debe juzgar cuales observaciones son materiales a diversos niveles de la gerencia y se debe informar de acuerdo a ello.

f. Informe de auditoría.

Los informes de auditoría son el producto final del trabajo del auditor de sistemas, este informe es utilizado para indicar las observaciones y recomendaciones a la gerencia; aquí también se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoría, no existe un formato específico para exponer un informe de auditoría de sistemas de información, pero generalmente tiene la siguiente estructura o contenido:

- Introducción al informe, donde se expresara los objetivos de la auditoría, el período o alcance cubierto por la misma, y una expresión general sobre la naturaleza o extensión de los procedimientos de auditoría realizados.
- Observaciones detalladas y recomendaciones de auditoría.
- Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.
- Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

g. Seguimiento de las observaciones de auditoría.

El trabajo de auditoría es un proceso continuo. No serviría de nada el trabajo de auditoría si no se comprueba que las acciones correctivas tomadas por la gerencia, se están realizando. Para esto se debe tener un programa de seguimiento. La oportunidad de seguimiento dependerá del carácter crítico de las observaciones de auditoría. El nivel de revisión de seguimiento del auditor de sistemas dependerá de diversos factores; en algunos casos el auditor de sistemas tal vez solo necesite inquirir sobre la situación actual. En otros casos tendrá que hacer una revisión más técnica del sistema.

5.3.2. NTC-ISO/IEC 27001:2006

Entre los objetivos primordiales del estándar ISO/IEC 27001[13] se considera presentar un análisis para cualquier empresa que desee planificar e implementar una política de seguridad orientada a obtener una futura certificación dentro de este estándar y conseguir como resultado final la evaluación del riesgo (análisis y valoración) sobre las políticas empresariales de una organización.

El alcance se concibe hasta proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

La adopción del modelo SGSI obedece a una decisión estratégica de la organización, pues el modelo está influenciado por sus necesidades y objetivos, así como por los requerimientos de

[13] Principales estándares para la seguridad de la información IT. Alcances y consideraciones esenciales de los estándares. Flor Nancy Díaz Piraquive. Revista Eos No.2, 2008.

seguridad, los procesos, el tamaño y la estructura de la empresa. La dinámica que implica su aplicación ocasionará en muchos casos la escala del modelo, por lo que se necesita una misma dinámica para las soluciones.

Los requerimientos de la NTC-ISO/IEC 27001:2006 son aplicables a todas las organizaciones.

5.3.2.1. Modelo PHVA

Adoptado por la NTC-ISO/IEC 27001:2006

- *Planear (establece el SGSI):* Fija la política, objetivos, procesos y procedimientos del SGSI pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados conforme a las políticas y objetivos generales de la organización.
- *Hacer (implementar y operar el SGSI):* mplementar y operar la política, controles, procesos y procedimientos del SGSI.
- *Verificar (monitorear y revisar el SGSI):* Evaluar y, donde corresponda, medir el desempeño del proceso según la política, objetivos y experiencia práctica del SGSI, e informar los resultados a la gerencia para su examen.
- *Actuar (mantener y mejorar el SGSI):* omar medidas correctivas y preventivas, basado en los resultados de la auditoría interna del SGSI y el examen de la gerencia u otra información pertinente, para lograr el mejoramiento continuo del SGSI.

El modelo PHVA establece para el SGSI un procedimiento que tenga en cuenta la definición del alcance de un enfoque sistemático para identificar y evaluar el riesgo, definir política SGSI, identificar y evaluar opciones para el tratamiento del riesgo, seleccionar objetivos de control y controles, preparar un enunciado de aplicabilidad y obtener aprobación de la gerencia.

De la misma manera, para la implantación y operación del SGSI considera tener en cuenta el formular e implementar un plan de tratamiento del riesgo, aplicar todos los objetivos de control y los controles seleccionados, poner en práctica programas de entrenamiento y toma de conciencia, al igual que gestionar operaciones y recursos.

Para monitorear y revisar el SGSI se recomienda ejecutar procedimientos de monitoreo, efectuar revisiones regulares de la eficacia del SGSI, revisar el nivel de riesgo residual y del riesgo aceptable, conducir las auditorías internas del SGSI y registrar todos los eventos que tienen un efecto en el desempeño del SGSI.

Para mantener y mejorar el SGSI, se necesita implantar las mejoras identificadas, tomar apropiadas acciones correctivas y preventivas, comunicar los resultados a todas las partes interesadas y asegurar que las mejoras alcancen los objetivos deseados.

En cuanto a documentación, ésta deberá incluir los registros de las decisiones de la gerencia, asegurar que las acciones se deriven de las decisiones y políticas de los directivos, y que los resulta-dos registrados sean reproducibles. Es importante poder demostrar que los controles seleccionados se relacionan con los resultados del proceso de evaluación y tratamiento de riesgos, y con la política y objetivos del SGSI.

5.3.3. NTC-ISO/IEC 27002:2007

El estándar internacional[14] fue publicado por la **ISO** y la **IEC**, que establecieron el comité técnico mixto **ISO/IEC JTC 1**. La fuente histórica para el estándar fue **BS 7799-1**, cuyas partes esenciales fueron tomadas en el desarrollo de la norma **ISO/IEC 17799:2005 "Tecnología de la Información ? Código de Prácticas para la Gestión de Seguridad de la Información"**. El estándar original inglés se publicó en dos partes:

- **BS 7799 Parte 1:** Tecnologías de la Información - Código de Prácticas para la Gestión de Seguridad de la Información.
- **BS 7799 Parte 2:** Sistemas de Gestión de Seguridad de la Información - Especificaciones con guías para su uso.

La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005; para la Colombia, su actualización se publico en noviembre de 2007 y se conoce como **NTC-ISO/IEC 27002:2007**. Se puede clasificar como las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002. A menudo se utiliza ISO/IEC 27002 como un término genérico para describir lo que actualmente son dos documentos diferentes:

- **ISO/IEC 17799 (ahora renombrada como ISO/IEC 27002):** Un conjunto de controles de seguridad (un código de práctica).
- **ISO/IEC 27001 (anteriormente, BS 7799?2):**Una especificación estándar para un sistema de gestión de seguridad de información (SGSI).

El objetivo del estándar NTC-ISO/IEC 27002:2007 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser

[14] Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa. Un reporte para gestión del ITGI y la OGC. IT GOVERNANCE INSTITUTE. [En línea], *http://www.ISACA.com/*

visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones inter-organizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

Los principios rectores en la norma NTC-ISO/IEC 27002:2007 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son:

- La protección y la no divulgación de datos personales.
- Protección de la información interna.
- Protección de los derechos de propiedad intelectual.

Las mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información.
- Asignación de la responsabilidad de seguridad de la información.
- Escalamiento de problemas.
- Gestión de la continuidad del negocio.

Cuando se implementa un sistema de gestión de seguridad de la información, se deben considerar varios factores críticos de éxito:

- La política de seguridad, sus objetivos y actividades deberían reflejar los objetivos de negocio.
- La implementación debería considerar los aspectos culturales de la organización.
- Se requiere un abierto apoyo y el compromiso de la alta dirección.
- Se requiere un conocimiento exhaustivo de los requisitos de seguridad, evaluación del riesgo y gestión del riesgo.
- El marketing efectivo de la seguridad debe dirigirse a todo el personal, incluidos los miembros de la dirección.

- La política de seguridad y las medidas de seguridad deben ser comunicadas a terceros contratados.
- Los usuarios deben ser capacitados en forma adecuada.
- Se debería disponer de un sistema integral y balanceado para la medición del desempeño, que apoye la mejora continua de suministro de información.

Después de presentar información introductoria (ámbito de aplicación, términos y definiciones), se debe presentar un marco de trabajo para el desarrollo de un Sistema de Gestión de Seguridad de Información específico para la empresa, que debería consistir de al menos los siguientes componentes:

- La política de seguridad.
- Organización para la seguridad.
- Clasificación de activos y su control.
- Seguridad del personal.
- Seguridad física y ambiental.
- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de la continuidad del negocio.
- Cumplimiento.

5.3.4. BIZAGI

BizAgi[15] es una solución de Business Process Management (BPMS) para una automatización de procesos más rápida y flexible. La Suite de BPM ha sido diseñada para resolver problemas de negocio reales.

Bizagi ofrece 2 productos complementarios: El Modelador de Procesos BPMN y BizAgi BPM Suite. Utilice el Modelador gratuito para documentar y diagramar sus procesos; luego oprima el botón Ejecutar para exportar el proceso a Bizagi BPM Suite, donde un asistente lo acompañará por todos los pasos necesarios para automatizar el proceso y convertirlo en una aplicación ejecutable (workflow).

[15] BizAgi. BizAgi BPM Suit. [En línea], *http://www.bizagi.com*

BizAgi es la solución de BPM que le permitirá modelar, ejecutar y mejorar sus procesos de negocio a través de un entorno gráfico y sin necesidad de programación.

Funcionamiento

El concepto de la BizAgi BPM trata sobre la generación automática de una aplicación web, la cual está basada y activada mediante un diagrama de proceso sin que se requiera alguna programación, donde el proceso es la aplicación. Para lograrlo, la Suite BizAgi BPM maneja el ciclo completo de vida de un proceso de negocio: Modelar, Automatizar, Ejecutar, y Mejorar. Cada una de estas fases están manejadas por componentes diferentes, que permiten, mediante el uso de un ambiente gráfico y dinámico, la construcción de una solución basada en procesos.

Los pasos para construir una solución BizAgi consta de:

- **Modelar:** El primer paso para crear soluciones en Bizagi es determinar los procesos. Para hacer esto se cuenta con el Modelador de Procesos BizAgi. El Modelador de Procesos Bizagi permite diagramar y documentar procesos de una forma ágil y simple. Éste a su vez, presenta los procesos de negocio usando un estándar aceptado mundialmente, el cual es más comúnmente conocido como BPMN (Business Process Modeling Notation).
- **Automatizar:** Luego del diseño de procesos, el siguiente paso es automatizar. Aquí se convierten todas las actividades de proceso en una aplicación tecnológica. BizAgi ofrece un conjunto de herramientas que gráficamente genera un modelo asociado a un proceso de negocio (diagrama de flujo, reglas de negocio, interfaz de usuario, etc.). Este modelo es almacenado en una base de datos, y es interpretado y ejecutado en producción a través de una aplicación web mediante el servidor BPM sin la necesidad de código. La aplicación web resultante, luego del proceso de automatización, tiene una característica muy importante: cuando el proceso es modificado (cualquier elemento del modelo) la aplicación web muestra los cambios automáticamente.
- **Ejecutar:** El servidor de BizAgi BPM es el motor que ejecuta y controla los procesos de negocio construidos en BizAgi Studio. Este servidor está basado en una colección de componentes que ofrecen todas las funcionalidades necesarias para una administración efectiva de procesos de negocio (portal de trabajo, BAM, reglas de negocio, motor de integración, etc.). El servidor BPM, basado en el modelo previamente construido, vela por la exactitud y la adecuación de la ejecución en las distintas tareas y actividades que intervienen en el proceso de negocio; mediante el control y la verificación de tareas terminadas en el momento correcto, por la persona o recurso correcto, y de acuerdo a los lineamientos, objetivos y otras reglas fundamentales a considerar.
- **Mejorar:** El Servidor BPM de BizAgi tiene un conjunto completo de reportes de rendimiento e indicadores sobre los procesos que le permitirán analizar los procesos de negocio, identificar cuellos de botella y sus causas, e identificar oportunidades de mejora en ellos. Basado en los resultados, los procesos y políticas pueden ser ajustados en

tiempo real usando la aplicación web. Las mejoras pueden ser hechas también, usando Bizagi Studio para generar una nueva versión del proceso. Esta nueva versión del proceso puede ser puesta en producción sin que se requiera algo de programación, en un periodo de tiempo corto, tan solo modificando el modelo de negocio la aplicación se adaptará automáticamente, haciéndolo fácil para hacer mejoras continuas y para incrementar la productividad.

5.3.5. BonitaSoft

Descripción.[16]

BonitaSoft es una solución de código abierto para la gestión de procesos de negocios. El gestor permite:

- Colaborar, para vincular a los analistas de negocio con el equipo de TI durante el proceso de modelado. El estándar BPMN brinda la facilidad de modelar un proceso en equipo.
- Desarrollar, que comprende desde el diseño de un proceso hasta lograr una aplicación completa.
- Construir y probar los modelos de procesos en entornos reales. Así mismo, puede simular y evaluar modelos alternativos para optimizar sus procesos.
- Monitorizar, con funciones y generación de informes para garantizar que las personas y los procesos operen con la máxima productividad.
- Conectar, con su amplia variedad de conectores se pueden enlazar procesos con sistemas de información ya existentes con el mínimo de código personalizado.
- Desplegar, con la capacidad de desarrollar arquitecturas complejas en clústeres y de conectarse al Portal de Bonita BPM desde su PC o a través de dispositivos móviles.

Funcionamiento[17]

Bonita BPM combina tres herramientas en una para la automatización de procesos de negocio: un innovador Studio de diseño de procesos, un potente motor de ejecución de procesos y una interfaz de usuario sencilla y fácil de utilizar.

[16] BonitaSoft. Bonita BPM 6.4. [En línea], *http://es.bonitasoft.com/*
[17] BonitaSoft. Bonita BPM 6.4. [En línea], *http://es.bonitasoft.com/*

- ***Bonita Studio:***
  Bonita BPM Studio permite diseñar fácilmente un modelo de proceso ejecutable con BPMN2. Con el Studio podemos:

  - Diseñar procesos sbre una pizarra, facilitando el desafío de implementar el estándar *"Notación para el Modelado de Procesos de Negocio"* (**BPMN** or **Business Process Management Notation**) con una herramienta gráfica sencilla de usar.
  - Cconectar fácilmente sus sistemas de información, al integrar un amplio panel de conectores listos para usar a: base de datos, mensajería, ERP, ECM, data warehouse, CRM, entre otros. En caso de no encontrar lo que necesita, puede crear fácilmente nuevos conectores y compartirlos con la comunidad Open Source de Bonitasoft.
  - Construya y personalice sus aplicaciones con mini-aplicaciones (widgets) de tipo "arrastrar y soltar", donde se cuenta con listas de selección, botones de opción, etc., para crear formularios que correspondan a las etapas del procesoen desarrollo. También puede optimizar la visualización de sus formularios en unos clics e importar modelos para adaptar sus aplicaciones a la identidad visual que desee.

- ***Bonita Portal:***
  La gran capacidad de personalización de la interfaz del usuario final, tanto para versión móvil como desktop, permiten la actualización en ejecución de los procesos gestionando los errores en directo, logrando así fluidez de manera correcta en las aplicaciones. Portal Bonita BPM permite:

  - Ejecutar sus aplicaciones en un solo clic, un sólo clic basta para generar la aplicación basada en los procesos de negocio, luego sólo queda desplegarla. Una vez terminado el modelado de los procesos y la conectividad establecida con los sistemas de información, puede personalizar los formularios y generar la aplicación de negocio en un sólo clic.
  - Monitorear los procesos, pensado para ser tan simple el uso como un gestor de correo; el portal Bonita permite la ejecución de procesos de manera intuitiva. Provee una vista global de los trámites en curso para un mejor monitoreo de los procesos.
  - Gestionar fácil y rápidamente las tareas de usuario para organizar el trabajo, colaborar con el equipo, los clientes y proveedores, controlando gráficamente el estado de los procesos.

- ***Bonita Engine:***
  El motor de Bonita BPM maneja con facilidad grandes procesos de alta demanda con transacciones de gran volumen en entornos complejos. La flexibilidad del motor de ejecución de Bonita le permite adaptarse a todo tipo de arquitectura de sistemas de información, del más sencillo al más complejo.

Ediciones[18]

[18] BonitaSoft. Bonita BPM 6.4. [En línea], *http://es.bonitasoft.com/*

Actualmente Bonita cuenta con cuatro (4) ediciones:

- ***Community:*** Es una suite open source para la gestión de procesos de negocio. Es la edición gratuita de Bonita. ideal para el desarrollador que desea adquirir la competencia profesional para crear potentes aplicaciones de procesos de negocio. Con esta suite se puede:

  - Construir la aplicación de negocio en el Bonita BPM Studio.
  - Gestionar un número ilimitado de tareas de proceso con el Bonita BPM Engine.
  - Utilizar el Bonita BPM Portal para completar el trabajo.

- ***Teamwork:*** Ideal para crear aplicaciones de negocio independientemente del tamaño de la empresa. Es una de las ediciones por suscripción. Además de incorporar las funcionalidades de la edición Community, Teamwork permite:

  - Diseñar formularios web dinámicos.
  - Usar herramientas de integración avanzadas.
  - Usar herramientas para desarrollo colaborativo.
  - Definit y administrar los datos de negocio.

- ***Efficiency:*** Permite crear y gestionar aplicaciones de negocio totalmente personalizables para móviles y web. Al igual que la edición Teamwork, es brindada por suscripción. Incorpora las funcionalidades del Teamwork y las siguientes:

  - Crear aplicaciones web propias.
  - Construir aplicaciones moviles personalizadas.
  - Supervisar el estado en tiempo real de las aplicaciones de negocio.

- ***Performance:*** Es el BPM definitivo, el cual no cuenta con límites para las aplicaciones de negocio críticas. Esta edición, de la mism manera como la Teamwork y la Efficiency, es brindada por suscripción. Incorpora las funcionalidades de la edición Efficiency y además de las siquientes:

  - Actualizar parámetros en tiempo de ejecución.
  - Solucionar y relancer las tareas fallidas.
  - Una plataforma que da servicio a multiples organizaciones.
  - Definir una arquitectura en cluster para asegurar una alta disponibilidad.

Las ediciones por suscripciones son ideales para equipos de desarrolladores que colaboran para resolver problemas técnicos o de negocio mejorando las aplicaciones de procesos de negocio. Las tres ediciones de este tipo son de pago; sin embargo, cuantan con un periodo de prueba de treinta días para usar sus funcionalidades.

5.3.6. Spring Framework

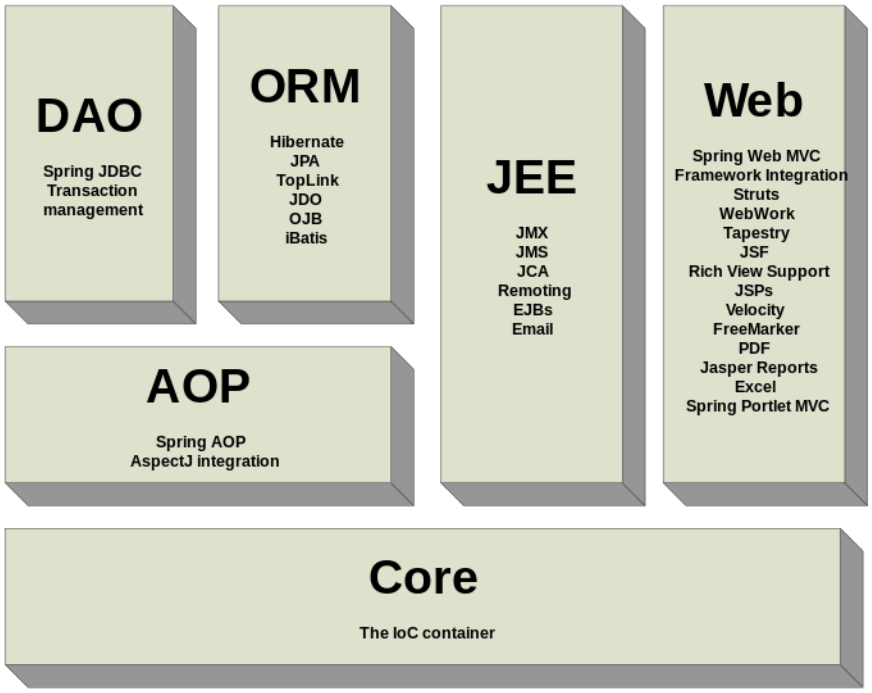
Spring[19] es un contenedor ligero para la construcción de aplicaciones empresariales, el cual proporciona un soporte comprensivo para el desarrollo de sistemas. Spring es un framework modular,lo que permite utilizar solo lo necesario; además, no es intrusivo, lo cual significa fácil integración en los proyectos y promueve el desarrollo con una alta cohesion (especialización de clases) y bajo acoplamiento (código menos dependiente).//

5.3.6.1. Funcionamiento

Spring Framework esta compuesto de varias características; se encuentra organizado en 20 módulos independientes, tal y como se aprecia en la siguiente imagen:

[19] Introducción a Spring Framework. [Online]: *https://jaehoo.wordpress.com/2010/11/28/introduccion-a-spring-framework/*

Figura 5.1: *Visión general de Spring Framework. Componentes.*



Fuente: *https://jaehoo.wordpress.com/2010/11/28/introduccion-a-spring-framework/*

METODOLOGÍA

6.1. TIPO DE INVESTIGACIÓN

Se realiza un estudio cuantitativo.

6.2. POBLACIÓN

Para la población, se toman todos los procesos que intervienen en el proceso de auditoría en seguridad de la información vinculados con el anexo A de la norma NTC-ISO/IEC 27001:2006.

6.3. MUESTRA

Para la muestra, se eligen los procesos que intervienen en el proceso de auditoría en seguridad de la información vinculados a los dominios A.6, A.8, A.13 y A.14 de la norma NTC-ISO/IEC 27001:2006.

6.4. VARIABLES

Las siguientes, son las variables tenidas en cuenta para evaluar la hipótesis, las cuales fueron usadas para medir cada uno de los procesos que intervienen en el proceso de auditoría de seguridad de la información vinculados a los a los dominios A.6, A.8, A.13 y A.14 de la norma NTC-ISO/IEC 27001:2006 y se describen a continuación:

- **Completo:** Lista de chequeo de los controles implementados en los anexos A.6, A.8, A.13 y A.14 de la norma ISO 27001 para un proceso de auditoría de seguridad de la información.
- **Facilidad de uso:** Se cataloga la facilidad de uso de la herramienta implementada por parte del usuario.
- **Claridad del procedimiento:** Se evalúa la claridad en el proceso de auditoría de seguridad de la información al usar la herramienta para llevarla a cabo.Tiempo de respuesta para el ingreso de los datos: Tiempo que tarda el usuario para registrar en la herramienta las conformidades, no conformidades, observaciones y demás que se consideren necesarias durante un proceso de auditoría de seguridad de la información.

- **Tiempo de elaboración del informe:** Valor consolidado del tiempo que tarda la herramienta en generar el reporte y, posteriormente, el informe de auditoría de seguridad de la información.
- **Tiempo de generación del reporte:** Tiempo que tarda la herramienta en generar el reporte preliminar del proceso de auditoría de seguridad de la información.
- **Tiempo de generación de informe:** Tiempo que tarda la herramienta para generar el informe de auditoría de seguridad de la información.

6.5. DISEÑO DE INSTRUMENTOS PARA TOMA DE INFORMACIÓN

Antes de iniciar el diseño de los instrumentos de medición, fue necesario realizar un análisis de los dominios de la norma NTC-ISO/IEC 27001:2006 objeto de estudio: *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"*, respectivamente. Así mismo, fue necesario revisar las pautas de implementación de cada uno de los controles de los dominios mencionados, tal y como se contempla en la NTC-ISO/IEC 27002:2007, para identificar las actividades relevantes y las pautas a tener en cuenta cuando se quiere implementar,lo cual permita predeterminar las acciones a seguir por parte del auditor interno.

Una vez realizado el análisis y contar con un listado de actividades por cada control, se realiza el modelado del proceso de auditoría en seguridad de la información para los dominios objetivo. el modelado se lleva a cabo desde el nivel más general hasta lo más específico, los cuales se aprecian en apartados posteriores. Con el proceso modelado, se genera un documento con las entradas, actividades, salidas y recomendaciones de cada dominio de control a evaluar, puesto en consideración por parte de expertos en seguridad de la información, con el fin de determinar si se considera necesario o no realizar ajustes en el modelo propuesto. Para llevar a cabo validación por parte de los expertos, se ha estructurado el siguiente formulario de encuesta:

EVALUACIÓN DE CUMPLIMIENTO Y CLARIDAD PARA PROCESO DE AUDITORÍA INTERNA EN SEGURIDAD DE LA INFORMACIÓN ASOCIADO A LOS ASPECTOS DE LOS DOMINIOS 6, 8, 13 Y 14 DEL ANEXO A DE LA NORMA NTC-ISO/IEC 27001:2006

Objetivo: *Medir el nivel de cumplimiento respecto a la norma ISO 27001 en su versión 2006 y claridad del proceso de auditoría propuesto para los dominios 6, 8, 13 y 14 del anexo A de la norma* ***NTC-ISO/IEC 27001:2006****.*

1. CUMPLIMIENTO RESPECTO A LA NORMA ISO 27001:2006

Para medir el nivel de cumplimiento del proceso de auditoría interna con base en la norma se debe calificar cada indicador de los aspectos en una escala de ***0*** *a* ***5****, siendo 0 no cumple y 5 cumple completamente:*

Tabla 6.1: ***Cumplimiento con base a la norma ISO 27001:2006***

CUMPLIMIENTO CON BASE EN LA NORMA ISO 27001							
OBJETIVO DE CONTROL	OBJETIVO	5	4	3	2	1	0
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN							
Organización interna	Gestionar la seguridad de la información dentro de la organización.						
Partes externas	Mantener la seguridad de la información de la organización y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstos.						
SEGURIDAD DE LOS RECURSOS HUMANOS							
Antes de la relación laboral	Asegurar que los empleados, contratistas y usuarios por tercera parte entiendan sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.						
Durante la relación laboral	Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, al igual que reducir el riesgo de error humano.						

Sigue en la página siguiente.

CUMPLIMIENTO CON BASE EN LA NORMA ISO 27001							
OBJETIVO DE CONTROL	OBJETIVO	5	4	3	2	1	0
Terminación o cambio de la relación laboral	Asegurar que los empleados, contratistas y usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.						
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN							
Reporte de eventos y debilidades de seguridad de la información	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.						
Gestión de incidentes y mejoras en la seguridad de la información	Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.						
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							
Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	Contrarrestar las interrupciones de las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.						

Fuente: *Autor*

2. CLARIDAD DEL PROCEDIMIENTO DE AUDITORÍA INTERNA

Para medir si el procedimiento de auditoría interna es claro, calificar para cada objetivo de control en una escala de ***0*** *a* ***5****, siendo 0 no claro y 5 totalmente claro:*

Tabla 6.2: ***Claridad del procedimiento de auditoría en seguridad de la información.***

CLARIDAD DEL PROCEDIMIENTO DE AUDITORÍA							
OBJETIVO DE CONTROL	OBJETIVO	5	4	3	2	1	0
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN							
Organización interna	Gestionar la seguridad de la información dentro de la organización.						
Partes externas	Mantener la seguridad de la información de la organización y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstos.						

Sigue en la página siguiente.

CLARIDAD DEL PROCEDIMIENTO DE AUDITORÍA							
OBJETIVO DE CONTROL	OBJETIVO	5	4	3	2	1	0
SEGURIDAD DE LOS RECURSOS HUMANOS							
Antes de la relación laboral	Asegurar que los empleados, contratistas y usuarios por tercera parte entiendan sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.						
Durante la relación laboral	Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, al igual que reducir el riesgo de error humano.						
Terminación o cambio de la relación laboral	Asegurar que los empleados, contratistas y usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.						
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN							
Reporte de eventos y debilidades de seguridad de la información	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.						
Gestión de incidentes y mejoras en la seguridad de la información	Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.						
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO							
Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	Contrarrestar las interrupciones de las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.						

Fuente: *Autor*

OBSERVACIONES:

Una vez validado el modelo, se procede a realizar el modelo de la arquitectura que se propondrá para automatizar el proceso de auditoría interna.

Al mismo tiempo, se realizará una prueba piloto con el proceso de auditoría con los ajustes propuestos por los expertos en una empresa de la región.

PROCESO DE AUDITORA INTERNA

7.1. CONSIDERACIONES GENERALES DE LOS PROCESOS DE AUDITORÍA INTERNA

7.1.1. Definición de procesos

Para levantar la información necesaria de cada uno de los procesos asociados a los cuatro aspectos objeto de estudio, se toma como modelo el siguiente formato[1]:

Tabla 7.1: ***Descripción general de procesos***

NOMBRE DEL PROCESO
TIPO DE PROCESO:
En este apartado se indica si el proceso es principal o de soporte.
ENTRADAS DEL PROCESO:
En este apartado se deben incluir los documentos y/o elementos necesarios para ejecutar el proceso.
OBJETIVOS DEL PROCESO:
Se debe describir de forma precisa y concreta cuál(es) el(los) objetivo(s) que se pretenden conseguir al ejecutar el proceso.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
En esta sección se realiza la descripción general del proceso y se especifican las actividades que hacen parte del mismo.
RESPONSABLE(S):
En este apartado se indica quién(es) es(son) el(los) responsable(s) de ejecutar el proceso y verificar que se realice correctamente.
PARTICIPANTES:
Aquí se indican las personas que se requieren que participen en la ejecución del proceso.
PROCESOS DE SOPORTE ASOCIADOS:
En este apartado se indica si el proceso tiene procesos de soporte asociados y en el caso que se tenga se define un nuevo formato para especificarlos independientemente.
DIAGRAMA DEL PROCESO:
En esta sección se incluye el diagrama del proceso realizado en una herramienta de modelamiento por procesos.
SALIDA DEL PROCESO:
Aquí se describen los diferentes documentos o elementos que se obtienen después de ejecutar el proceso.

[1]Paula A. Villa S. DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TIC'S. Universidad Tecnológica de Pereira, 2011. Pág. 38.

OBSERVACIONES:
En esta sección se especifican consideraciones y observaciones importantes para ejecutar el proceso.

Fuente: *Tabla 7.1: Descripción general de procesos. Paula Andrea Villa Sánchez. Definición de procesos de auditoría interna del sistema de gestión de seguridad de la información soportado en TIC. Trabajo de grado para optar al título de Especialista en redes de datos. Universidad Tecnológica de Pereira. 2011.*

7.1.2. Comparativo

Para realizar el modelado de cada uno de los procesos asociados a los dominios 6, 8, 13 y 14 del Anexo A de la norma ISO 27001 fue necesario realizar un comparativo tomando como insumo tres listas de checkeo: ***BS 7799.2:2002 Audit Check List (SANS)***, ***ISMS Auditing Guideline (ISO 27001 Implementer's Forum)*** e ***ISO 27002:2005***.

Tabla 7.2: ***Comparativo de listas de chequeo***

Anexo ISO 27001	**BS 7799.2:2002 Audit Check List (SANS)**	**ISMS Auditing Guideline (ISO 27001 Implementer's Forum)**	**ISO 27002**
6			

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
6.1		* Identificar las unidades de negocio (BU) de la estructura del SGSI y principales contactos para la auditoría. + Alto directivo responsable de TI y del SGSI. + Profesionales de seguridad de la información. + Supervisor de seguridad física y sitio y facilidades de contacto. + Contacto de recurso humano. + Administradores de sistemas y redes, arquitectos de seguridad y otros profesionales de TI. * Revisar la estructura de SGSI: + ¿En el SGSI se da suficiente énfasis (o hay una "fuerza impulsora") y un apoyo a la gestión? + ¿Hay un foro de gestión de alto nivel para discutir las políticas, riesgos y cuestiones del SGSI? + ¿Las funciones y responsabilidades son claramente definidas y asignadas a individuos calificados? + ¿Existe un presupuesto para las actividades del SGSI? + ¿Hay suficiente coordinación tanto dentro como entre las BU y con la sede? + ¿Los flujos de información (como notificaciones de incidentes) está operando en la práctica de manera efectiva?	Objetivo: Gestionar la seguridad de la información dentro de la Organización. Principios: * Establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información. * La política de seguridad de la información debe ser aprobada la dirección. Así mismo, debe asignar las funciones de seguridad, coordinar y revisar su implementación. * Solicitar el acceso a una fuente de asesoría especializada en seguridad de la información. * Debe promoverse la seguridad de la información con un enfoque multidisciplinario.
6.1.1			Mantener la seguridad de la información de la organización y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstos.
6.1.2	Sobre la existencia de un foro multifuncional de representantes de la dirección de las partes pertinentes de la organización para coordinar la aplicación de los controles de seguridad de la información.		Coordinadas las actividades para la seguridad de la información.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
6.1.3	Ya sea que la responsabilidad de la protección de los activos de las personas y para la realización de los procesos de seguridad específicos se define con claridad.		Definir claramente todas las responsabilidades para la seguridad de la información.
6.1.4	Si hay un proceso de autorización de gestión en el lugar para cualquier nueva instalación de procesamiento de información. Esto debe incluir todas las nuevas instalaciones, tales como hardware y software.		Definir y establecer un proceso de gestión de autorizaciones para el tratamiento de la información.
6.1.5	Asegurar que los empleados, contratistas y usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.		Identificar y revisar regularmente los acuerdos de confidencialidad o no divulgación de la información de la Organización.
6.1.6			* Mantener los contactos apropiados con las autoridades pertinentes. * Se debe contar con procedimientos que especifiquen el cuándo y a través de que autoridades se deben reportar los incidentes identificados en seguridad de la información o si se sospecha de incumplimiento de la ley.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
6.1.7	Sobre la existencia de un foro de gestión para asegurar que haya una dirección clara y visible apoyo a la gestión de las iniciativas de seguridad de la organización. Si se obtiene asesoramiento seguridad de la información especializada en su caso. Un individuo específico puede ser identificado para coordinar en - conocimientos y experiencias para garantizar la coherencia y proporcionar ayuda en la toma de decisiones de seguridad de la casa.		Mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.
6.1.8	Si la aplicación de la política de seguridad se revisa de forma independiente de manera regular. Esta es garantizar que las prácticas organizacionales reflejan adecuadamente la política, y que es factible y eficaz.		Revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
6.2		* Determinar las medidas para detectar e implementar en el SGSI requisitos para conexiones con tercera parte. + ¿Existe un proceso de análisis de riesgos en marcha para las conexiones de comunicación con tercera parte? + ¿Quién tiene la responsabilidad de velar porque todos los vínculos con tercera parte son, de hecho, identificados y evaluados los riesgos? + ¿Se mantiene un registro completo de las conexiones y módems de tercera parte autorizadas? + ¿Los arreglos de SGSI están en funcionamiento sobre las conexiones críticas rutinarias de tercera parte respecto a los requisitos? + ¿Existen contratos formales que cubren enlaces de tercera parte? Si es así, ¿se cubren aspectos de SGSI? + En su caso, ¿el contrato de outsourcing aborda adecuadamente los siguientes aspectos? - Propiedad y la responsabilidad en temas de SGSI. - Requisitos legales. - Protección de los sistemas, redes y datos a través de controles físicos, lógicos y procedimentales. - El derecho a una auditoría por parte de la organización.	Objetivo: Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros. Principios: * La seguridad de la información y las instalaciones de procesamiento de la información no deben ser reducidas por la introducción de un servicio o producto externo. * Controlar el acceso de terceros a los dispositivos de tratamiento de información. * En caso de requerirse un acceso de terceros, se debe realizar una evaluación de sus implicaciones sobre la seguridad y las medidas de control que requieren. Definir y aceptar las medidas por medio de un contrato con la tercera parte.
6.2.1	Si los riesgos de acceso de partes externas son identificados y controles de seguridad apropiados implementados. Si se identifican los tipos de accesos, que se clasifica y las razones de acceso están justificadas.		Identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a partes externas. * Implementar controles apropiados para conceder el acceso a partes externas.
6.2.1	Ya sea que los riesgos de seguridad con los contratistas de partes externas en el sitio de trabajo se identifican y controles apropiados se aplican.		

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
6.2.2	Sobre la existencia de un contrato formal que contenga, o, todos los requisitos referentes a seguridad a asegurar el cumplimiento con las políticas y estándares de seguridad de la organización.		Anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.
6.2.3	Si los requisitos de seguridad se abordan en el contrato con el tercero, cuando la organización ha subcontratado la gestión y el control de la totalidad o parte de sus sistemas de información, redes y / o entornos de escritorio. El contrato debe abordar cómo se quieren alcanzar, como se mantienen la seguridad y probaron los activos de la organización, y el derecho de la auditoría, las cuestiones de seguridad física y la forma en que la disponibilidad de los servicios que se va a mantener en caso de desastres de los requisitos legales.		Cumplir con los requisitos de seguridad de la información relevantes al acceso, proceso, comunicación o gestión de la información, las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones por parte de terceras partes.
8			

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
8.1		* Determinar si los roles y las responsabilidades de seguridad de la información se definen en las descripciones de puestos, términos y condiciones de empleo, etc., específicos para el personal de seguridad de TI, administradores de sistemas y redes, directivos y usuarios finales en general. + ¿Hay confidencialidad adecuada y clausulas similares? + ¿El personal y los contratistas contratados en puestos sensibles son preseleccionados? (incluyendo la toma de referencias y autorización de seguridad, cuando proceda). + ¿Hay procesos de detección mejorada para el personal y los directivos en funciones particularmente sensibles o sitios. + ¿Existen políticas y procedimientos de recursos humanos adecuados, en especial aquellas que se relacionan directamente con las normas de seguridad de TI?	Objetivo: * Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. * Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios. Principios: * Las responsabilidades de la seguridad debe definirse antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo. * Se debe seleccionar adecuadamente los cargos para nuevos empleados dentro de la organización, especialmente los trabajos sensibles. * Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deben firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.
8.1.1	Si las funciones de seguridad y responsabilidades establecidas en la política de seguridad de la información de la Organización se documentan en su caso. Esto debe incluir las responsabilidades generales de aplicación o el mantenimiento de la política de seguridad, así como las responsabilidades específicas para la protección de los bienes particulares, o para la ampliación de los procesos o actividades de seguridad particulares.		Definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
8.1.2	Ya sea que se llevaron a cabo controles de verificación de personal permanente en el momento de solicitud de empleo. Esto debe incluir el carácter de referencia, la confirmación de la reclamó títulos académicos y profesionales y los controles de identidad independientes.		Realizar verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes, las cuales deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual van a tener acceso y los riesgos percibidos.
8.1.3	Si los términos y condiciones del empleo abarcan la responsabilidad del empleado de seguridad de la información. En su caso, estas responsabilidades pueden continuar por un período definido después del final del empleo.		Aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
8.2		* Revisar la conciencia, formación y los planes educativos de seguridad de la información. + ¿Los usuarios finales y la dirección reciben constantemente una formación adecuada en seguridad de la información, incluyendo los roles y responsabilidades, procedimientos de acceso (login), entre otros, en el contexto de capacitación general de los sistemas de TI? + Revisar los procedimientos disciplinarios.	Objetivo: Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos. Principios: * Definir las responsabilidades de la Dirección para garantizar la aplicabilidad de la seguridad de la información en todos los puestos de trabajo. * A todos los usuarios empleados, contratistas y terceras partes se les debe proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad. * Establecer un proceso disciplinario normal para gestionar las brechas en seguridad.
8.2.1			Requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad de la información en concordancia con las políticas y los procedimientos establecidos por la organización.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
8.2.2	Si todos los empleados de la organización y de los usuarios de terceros (en su caso) reciben una formación adecuada para la Seguridad de la Información y actualizaciones reglamentarias		Los empleados, contratistas y usuarios de terceros deben recibir entrenamiento apropiado y actualizaciones regulares en políticas y procedimientos organizacionales acordes con sus funciones laborales.
8.2.3	Sobre la existencia de un proceso disciplinario formal para los empleados que han violado las políticas y procedimientos de seguridad de la organización. Tal proceso puede actuar como elemento de disuasión a los empleados que de otro modo podrían sentirse inclinados a hacer caso omiso de los procedimientos de seguridad.		Diseñar un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.
8.3		Revisar las políticas, normas, procedimientos y directrices relativas a los elementos de seguridad de la información, como recuperación de activos de información, claves, eliminación de los derechos de accesos, entre otros.	Objetivo: Garantizar que los empleados, contratistas y terceras partes salen de la organización o cambian su contrato laboral de forma organizada. Principios: * Se deben establecer las responsabilidades para gestionar la salida de los empleados, contratistas o terceras personas de la organización, la devolución de todo el equipo a su cargo y la cancelación de todos los derechos de acceso. * Manejar los cambios en las responsabilidades y empleos de la organización cuando sea necesario dar por terminado el contrato laboral; en caso de nuevos empleos, seguir lo contemplado en el numeral 8.1.
8.3.1			Definir y asignar claramente las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste.

Sigue en la página siguiente.

Anexo ISO 27001	**BS 7799.2:2002 Audit Check List (SANS)**	**ISMS Auditing Guideline (ISO 27001 Implementer's Forum)**	**ISO 27002**
8.3.2			Devolución de todos los activos en posesión de empleados, contratistas y terceros a la finalización de su empleo, contrato o acuerdo.
8.3.3			Retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceras partes a la información y a las instalaciones de procesamiento de información una vez terminado el empleo, contrato o acuerdo, o ser revisada en caso de cambio.
13			
13.1		* Revisar los procedimientos para la presentación de informes de eventos y debilidades de seguridad. * Trazar el proceso usando una muestra de documentación, como registros de Help Desk, comparando lo sucedido realmente con las políticas, procedimientos y directrices. * Confirmar quienes deben informar sobre los eventos y debilidades de seguridad son conscientes de, y en el uso real, el proceso.	Objetivo: Asegurar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente. Principios: * Establecer un reporte formal de los eventos y de los procedimientos de escalada. * Difundir a todos los empleados, contratistas y usuarios terceros los procedimientos para informar los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos. * Exigir que sean reportados todos los eventos de seguridad de información y las debilidades lo tan pronto como sea posible al punto de contacto designado.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
13.1.1	Si existe un procedimiento de notificación formal, a denunciar los incidentes de seguridad a través de canales ement ges adecuadas tan pronto como sea posible.		Informar los eventos en la seguridad de información haciendo uso de los canales de gestión apropiados lo más pronto posible.
13.1.2	Si existe un procedimiento formal de notificación o guía para los usuarios, para informar debilidad en la seguridad, o las amenazas a los sistemas o servicios.		Exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en cuanto a la seguridad de los mismos.
13.1.2	Ya se han establecido procedimientos para reportar cualquier mal funcionamiento de software.		
13.2		* Revisar la evaluación o investigación, acción correctiva y las partes posteriores de los procesos para la gestión de incidentes de seguridad a oportunidades de mejora. + ¿La organización cuenta con un proceso de gestión de incidentes relativamente madura en marcha? + Por consiguiente, ¿los incidentes, mejoras del conocimiento de riesgos y los controles de seguridad se aprenden de forma proactiva? * Comprobar los registros relativos a incidentes recientes para nuevas evidencias.	Objetivo: Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de la información. Principios: * Establecer las responsabilidades y procedimientos de gestión para manejar los eventos y debilidades de la seguridad de la información una vez reportados. * Aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información. * Garantizar el cumplimiento de los requisitos legales cuando se requiera hacer levantamiento de evidencia.

Sigue en la página siguiente.

Anexo ISO 27001	**BS 7799.2:2002 Audit Check List (SANS)**	**ISMS Auditing Guideline (ISO 27001 Implementer's Forum)**	**ISO 27002**
13.2.1			Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de información.
13.2.2	Si existen mecanismos que permitan a los tipos, volúmenes y costos de incidentes y fallos que se deben cuantificar y supervisar.		Debe existir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información.
13.2.3	Si el proceso involucrado en la recolección de los datos se ajusta a las prácticas jurídicas y la industria.		Recolectar, retener y presentar la evidencia de un incidente de seguridad de la información, conforme a las reglas establecidas en la jurisdicción relevante, cuando una acción de seguimiento contra una persona u organización se implique acción legal.
14			

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
14.1		* Evaluar la forma en que la organización determina y satisface sus necesidades de continuidad de negocio. * Revisar las políticas, procedimientos, normas y directrices asociadas. * Determinar si los diseños apropiados de "alta disponibilidad" son empleados para sistemas de TI, redes, entre otras, de apoyo a los procesos críticos del negocio. * Verificar si los involucrados entienden los riesgos a los que está enfrentada la organización. * Identificar correctamente los procesos críticos y los activos asociados al negocio. * Identificar los impactos potenciales del incidente. * Mandato de controles preventivos, detección y corrección adecuados. * Evaluar los planes de continuidad de negocio, ejercicios de continuidad y pruebas, entre otros, mediante el muestreo y la revisión de la documentación de procesos, informes, etc. * Verificar que los acontecimientos que probablemente interrumpan los procesos de negocio sean identificados y evaluados rápidamente, generando actividades del tipo de recuperación de desastres. * Verificar que los planes se han establecido adecuadamente para mantener las operaciones de negocios o restaurarlos en plazos definidos después de la interrupción o fallo. + ¿Los planes toman en cuenta la identificación y el acuerdo de responsabilidades, la identificación del procedimiento de recuperación y restauración, documentación de procedimientos y pruebas o ejercicios regulares? * Verificar que haya un solo marco coherente para la planificación de la continuidad del negocio. * Verificar si el marco asegura que todos los planes son coherentes e identifican las prioridades para pruebas y mantenimientos. * Determinar si los planes de continuidad del negocio y el proceso de planificación, tomándolos como un conjunto,	Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los eventos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna. Principios: * Implantar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización, hasta un nivel aceptable mediante una combinación de controles preventivos y de recuperación. * Identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio. * Analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio * Desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. * Integrar la seguridad de información como parte del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización. * Incluir en el proceso de evaluación los controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
		son suficientes para satisfacer los requisitos de seguridad de la información señalados. * Verificar si los planes de continuidad del negocio son ejercidos y probados con regularidad para garantizar que están siendo actualizados y eficaces. * Verificar si los miembros de crisis y gestión de incidentes y equipos de recuperación y otro personal relevante tienen claro sus funciones y responsabilidades.	
14.1.1	Sobre la existencia de un proceso controlado para desarrollar y mantener la continuidad del negocio en toda la organización. Esto podría incluir un Plan de la continuidad del negocio, pruebas regulares y la actualización del plan, formular y documentar una estrategia de continuidad del negocio, etc.		Desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
14.1.2	Si los eventos que pueden causar interrupciones de procesos de negocio se identificaron ejemplo: fallas en los equipos, inundaciones e incendios. Ya sea que se haya llevado a cabo una evaluación de riesgos para determinar el impacto de estas interrupciones. Si un plan estratégico fue desarrollado en base a los resultados de la evaluación de riesgo para determinar un enfoque global de la continuidad del negocio.		Identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones, así como sus consecuencias para la seguridad de información.

Sigue en la página siguiente.

Anexo ISO 27001	BS 7799.2:2002 Audit Check List (SANS)	ISMS Auditing Guideline (ISO 27001 Implementer's Forum)	ISO 27002
14.1.3	Ya se han desarrollado planes para restaurar las operaciones comerciales dentro del marco de tiempo requerido después de una interrupción o falta de procesos de negocio. Si el plan se pone a prueba y se actualiza regularmente.		Desarrollar e implantar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y en la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.
14.1.4	Sobre la existencia de un único marco de un plan de continuidad del negocio. Si este marco se mantiene para asegurar que todos los planes sean coherentes y determinar las prioridades de prueba y mantenimiento. Si esto identifica las condiciones de activación y las personas responsables de la ejecución de cada componente del plan.		Mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimientos.
14.1.5	Si los planes de continuidad de negocios se ponen a prueba con regularidad para asegurarse de que están actualizados y eficaces. Si los planes de continuidad de negocios se mantuvieron mediante revisiones periódicas y actualizaciones para asegurar su eficacia constante. Si los procedimientos se incluirán en el programa de gestión del cambio a las organizaciones a asegurar que los asuntos de continuidad de negocio se tratan adecuadamente.		Someter a pruebas y revisiones periódicas en los planes de continuidad del negocio para asegurar su actualización y eficacia.

Fuente: *Autor*

El comparativo permite definir las actividades generales que el auditor debe realizar en una auditoría, obteniendo la siguiente tabla con las actividades asociadas a la pre-auditoría y au-

ditoría en sitio:

Tabla 7.3: ***Actividades generales, previas y en sitio de la auditoría.***

Anexo ISO 27001	**Actividad general**	**Previo**	**En sitio**
6			
6.1	¿Existe un presupuesto para las actividades del SGSI?		
6.1.1	* ¿Se da la importancia y apoyo suficiente a la gestión del SGSI? * ¿Se cuanta con un apoyo activo de la Dirección en las responsabilidades sobre seguridad de la información dentro de la Organización?	Revisar documento de compromiso y responsabilidades de la dirección con la seguridad de la información.	* ¿Se da la importancia y apoyo suficiente a la gestión del SGSI? * ¿Se cuenta con un apoyo activo de la Dirección en las responsabilidades sobre seguridad de la información dentro de la Organización?
6.1.2	* Verificar que las actividades para la seguridad de la información están coordinadas. + ¿Hay suficiente coordinación dentro y fuera de las BU de la organización? + ¿Existe un foro multifuncional de representantes de las partes interesadas de la organización para coordinar la aplicación de los controles de seguridad de la información?	Revisar documento donde se especifique las actividades de coordinación de la seguridad de la información al interior de la organización, así como donde se identifiquen a sus partes interesadas con los roles y responsabilidades pertinentes.	* Verificar que las actividades para la seguridad de la información están coordinadas. + ¿Hay suficiente coordinación dentro y fuera de las BU de la organización? + ¿Existe un foro multifuncional de representantes de las partes interesadas de la organización para coordinar la aplicación de los controles de seguridad de la información?
6.1.3	* Verificar si se definieron claramente todas las funciones y responsabilidades para la seguridad de la información. * ¿Las funciones y responsabilidades de seguridad de la información son asignadas a personal adecuado y calificado?	Revisar documento donde se especifiquen las funciones y responsabilidades del personal en lo referente a la seguridad de la información.	* Verificar si se definieron claramente todas las funciones y responsabilidades para la seguridad de la información. * ¿Las funciones y responsabilidades de seguridad de la información son asignadas a personal adecuado y calificado?
6.1.4	* Verificar si se define y establece un proceso de gestión de autorizaciones para el tratamiento de la información. + Si el proceso de autorización de gestión existe, verificar que se aplique para nuevas instalaciones de procesamiento de información, tales como hardware y software.	Revisar procedimiento de gestión de autorización de la dirección para las instalaciones de procesamiento de información.	* Verificar si se define y establece un proceso de gestión de autorizaciones para el tratamiento de la información. + Si el proceso de autorización de gestión existe, verificar que se aplique para nuevas instalaciones de procesamiento de información, tales como hardware y software.

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
6.1.5	* ¿A los empleados se les pide firmar un acuerdo de confidencialidad o de no divulgación como parte de sus condiciones iniciales del empleo? * ¿En el acuerdo firmado se hace referencia a la seguridad de las instalaciones de procesamiento de información y la organización de los activos? * Verificar si se identifica y revisa regularmente los acuerdos de confidencialidad o no divulgación de la información de la Organización.	? Revisar el documento firmado por los empleados donde se comprometen a guardar confidencialidad o no divulgación en cuanto a la protección de la información. * Revisar los registros de revisión de acuerdos de confidencialidad.	* ¿A los empleados se les pide firmar un acuerdo de confidencialidad o de no divulgación como parte de sus condiciones iniciales del empleo? * ¿En el acuerdo firmado se hace referencia a la seguridad de las instalaciones de procesamiento de información y la organización de los activos? * Verificar si se identifica y revisa regularmente los acuerdos de confidencialidad o no divulgación de la información de la Organización.
6.1.6	* ¿Se mantiene un contacto apropiado con las autoridades pertinentes? * ¿Se cuenta con un procedimiento de reporte de incidentes de seguridad de la información o sospecha de incumplimiento de la ley con la autoridad según corresponda?	Revisar procedimiento de contacto con autoridades.	* ¿Se mantiene un contacto apropiado con las autoridades pertinentes? * ¿Se cuenta con un procedimiento de reporte de incidentes de seguridad de la información o sospecha de incumplimiento de la ley con la autoridad según corresponda?
6.1.7	* ¿Se mantiene contacto con grupos o foros de seguridad de la información especializados y asociaciones profesionales para discutir las políticas, riesgos y cuestiones de SGSI? * ¿Existe un foro de gestión para asegurar que haya una dirección clara y visible apoyo a la gestión de las iniciativas de seguridad de la organización? * En su caso, ¿se cuenta con asesoramiento en seguridad de la información especializada? * ¿Se puede identificar a un responsable con los conocimientos y experiencias necesarios para garantizar coherencia y proporcionar ayuda en la toma de decisiones de seguridad de la empresa?	Revisar actas de reunión con grupos de interés especiales, otros foros especializados en seguridad de la información y asociaciones de profesionales.	* ¿Se mantiene contacto con grupos o foros de seguridad de la información especializados y asociaciones profesionales para discutir las políticas, riesgos y cuestiones de SGSI? * ¿Existe un foro de gestión para asegurar que haya una dirección clara y visible apoyo a la gestión de las iniciativas de seguridad de la organización? * En su caso, ¿se cuenta con asesoramiento en seguridad de la información especializada? * ¿Se puede identificar a un responsable con los conocimientos y experiencias necesarios para garantizar coherencia y proporcionar ayuda en la toma de decisiones de seguridad de la empresa?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
6.1.8	* Revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación. * ¿La gestión de seguridad de la información pasa por revisión independiente a intervalos planificados? * ¿Se realiza una revisión independiente de la gestión de la seguridad de la información cuando ocurren cambios significativos en el SGSI? * ¿Las personas que realizan las revisiones cuentan con la experiencia y las habilidades adecuadas?	* Revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación. * Revisar programa de auditorías en seguridad de la información por organismos independientes. * Revisar resultado de auditorías en seguridad de la información realizado por organismos independientes.	* ¿La gestión de seguridad de la información pasa por revisión independiente a intervalos planificados? * ¿Se realiza una revisión independiente de la gestión de la seguridad de la información cuando ocurren cambios significativos en el SGSI? * ¿Las personas que realizan las revisiones cuentan con la experiencia y las habilidades adecuadas?
6.2	* Determinar las medidas para detectar e implementar en el SGSI requisitos para conexiones con tercera parte.		
6.2.1	* ¿Existe un proceso de análisis de riesgos para las conexiones de comunicación con partes externas? + ¿Se tienen identificados los riesgos asociados a la seguridad la información de la organización que impliquen a partes externas? + ¿Se tienen implementados y se están aplicando los controles apropiados para conceder el acceso a partes externas? + ¿Se cuenta con un responsable para velar por todos los accesos con partes externas parte según los riesgos identificados y evaluados? * ¿Se tienen identificados los tipos de accesos, su clasificación y se justifican las razones para contar con cada uno de ellos? * ¿Los usuarios de partes externas tienen claros los riesgos de seguridad en el sitio de trabajo?	Revisar matriz de riesgos en seguridad de la información donde de se identifiquen los riesgos asociados a partes externas	* ¿Existe un proceso de análisis de riesgos para las conexiones de comunicación con partes externas? + ¿Se tienen identificados los riesgos asociados a la seguridad la información de la organización que impliquen a partes externas? + ¿Se tienen implementados y se están aplicando los controles apropiados para conceder el acceso a partes externas? + ¿Se cuenta con un responsable para velar por todos los accesos con partes externas según los riesgos identificados y evaluados? * ¿Se tienen identificados los tipos de accesos, su clasificación y se justifican las razones para contar con cada uno de ellos? * ¿Los usuarios de partes externas tienen claros los riesgos de seguridad en el sitio de trabajo?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
6.2.2	* Solicitar todos los requisitos de seguridad exigidos a los clientes antes de otorgar acceso a la información o a los activos de la organización. * ¿El SGSI contempla una política de control de acceso a la información de la empresa para clientes? * ¿Existe una descripción clara de los servicios disponibles para los clientes? * ¿Los clientes tienen claras sus responsabilidades, tanto civiles como legales, con la seguridad de la información de la empresa?	* Solicitar todos los requisitos de seguridad exigidos a los clientes antes de otorgar acceso a la información o a los activos de la organización. * Revisar procedimiento para permitir acceso a clientes a activos o información de la organización.	* ¿El SGSI contempla una política de control de acceso a la información de la empresa para clientes? * ¿Existe una descripción clara de los servicios disponibles para los clientes? * ¿Los clientes tienen claras sus responsabilidades, tanto civiles como legales, con la seguridad de la información de la empresa?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
6.2.3	* ¿El SGSI contempla una política de control de acceso a la información de la empresa por tercera parte? * ¿Existen contratos formales que cubren accesos de tercera parte a los sistemas de información de la empresa? Si es así, ¿se cubren también aspectos del SGSI? * Revisar estructura del contrato con terceras partes: + ¿Se especifican los requisitos legales, el alcance, el cómo se mantendrá la seguridad? + ¿Se identifican los activos de la organización involucrados? + ¿Se declara por escrito el derecho de auditar el proceso realizado por el contratista? + ¿Se consideran los aspectos de seguridad física? + ¿Se contempla la disponibilidad de los servicios que deben mantenerse en caso de desastres? * Cuando la organización subcontratara la gestión o implantación total o parcial de sus sistemas de información, redes o entornos de escritorio, ¿se cumplen con todos los requisitos en contratos con tercera parte? * Si la empresa maneja contratos de outsourcing, ¿se abordan adecuadamente los siguientes aspectos? + Propiedad y la responsabilidad en temas de SGSI. + Requisitos legales. + Protección de los sistemas, redes y datos a través de controles físicos, lógicos y procedimentales. + El derecho a una auditoría por parte de la organización. * ¿Existe una descripción clara de los servicios disponibles para las terceras partes, así como de la información que estará disponible y su clasificación de seguridad? * ¿Se mantiene un registro completo de las conexiones autorizadas con tercera parte?	? Revisar política y procedimiento para control de acceso a la información de la empresa por parte de tercera parte. * Revisar estructura del contrato con terceras partes, tanto de gestión o implementación total o parcial como de outsourcing. * Revisar documento donde se especifiquen los servicios disponibles a tercera parte. * Revisar registro de conexiones autorizadas a tercera parte.	* ¿El SGSI contempla una política de control de acceso a la información de la empresa por tercera parte? * ¿Existen contratos formales que cubren accesos de tercera parte a los sistemas de información de la empresa? Si es así, ¿se cubren también aspectos del SGSI? * En la revisión de la estructura del contrato con terceras partes: + ¿Se especifican los requisitos legales, el alcance, el cómo se mantendrá la seguridad? + ¿Se identifican los activos de la organización involucrados? + ¿Se declara por escrito el derecho de auditar el proceso realizado por el contratista? + ¿Se consideran los aspectos de seguridad física? + ¿Se contempla la disponibilidad de los servicios que deben mantenerse en caso de desastres? * Cuando la organización subcontratara la gestión o implantación total o parcial de sus sistemas de información, redes o entornos de escritorio, ¿se cumplen con todos los requisitos en contratos con tercera parte? * Si la empresa maneja contratos de outsourcing, ¿se abordan adecuadamente los siguientes aspectos? + Propiedad y la responsabilidad en temas de SGSI. + Requisitos legales. + Protección de los sistemas, redes y datos a través de controles físicos, lógicos y procedimentales. + El derecho a una auditoría por parte de la organización. * ¿Existe una descripción clara de los servicios disponibles para las terceras partes, así como de la información que estará disponible y su clasificación de seguridad? * ¿Se mantiene un registro completo de las conexiones autorizadas con tercera parte?
8			

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
8.1	* Determinar si los roles y las responsabilidades de seguridad de la información se definen en las descripciones de puestos, términos y condiciones de empleo, etc., específicos para el personal de seguridad de TI, administradores de sistemas y redes, directivos y usuarios finales en general.		
8.1.1	* Verificar si se definen y documentan los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información. + ¿Existen procesos que permitan asignar al personal y los directivos acceso a zonas sensibles según sus funciones? + ¿Existen políticas y procedimientos adecuados para el recurso humano, en especial con aquellos relacionados directamente con las normas de seguridad de TI? + ¿Se documentan las funciones y responsabilidades de seguridad establecidas en la política de seguridad de la información de la Organización? + ¿Se incluyen las responsabilidades para la aplicación o mantenimiento de la política de seguridad? + ¿Se incluyen las responsabilidades para la protección de los bienes o la ampliación de los procesos o actividades de seguridad específicos?	* Verificar si se definen y documentan los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información.	* ¿Existen procesos que permitan asignar al personal y los directivos acceso a zonas sensibles según sus funciones? * ¿Existen políticas y procedimientos adecuados para el recurso humano, en especial con aquellos relacionados directamente con las normas de seguridad de TI? * ¿Se documentan las funciones y responsabilidades de seguridad establecidas en la política de seguridad de la información de la Organización? * ¿Se incluyen las responsabilidades para la aplicación o mantenimiento de la política de seguridad? * ¿Se incluyen las responsabilidades para la protección de los bienes o la ampliación de los procesos o actividades de seguridad específicos?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
8.1.2	* ¿Se verifican los antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes? + ¿Al verificar los antecedentes de los candidatos se tienen en cuanta los requisitos del negocio, la clasificación de la información involucrada dentro de sus funciones y lo riesgos percibidos en el cargo? * ¿Es preseleccionado el personal y los contratistas contratados en puestos sensibles? * ¿Se llevan a cabo controles de verificación del personal en el momento de solicitud de empleo? * Con los contratistas y los usuarios de tercera parte, ¿en el contrato se especifican claramente las responsabilidades de las partes y los procedimientos de notificación para su selección?	? Revisar procedimiento para selección de personal.	* ¿Se verifican los antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes? * ¿Al verificar los antecedentes de los candidatos se tienen en cuanta los requisitos del negocio, la clasificación de la información involucrada dentro de sus funciones y lo riesgos percibidos en el cargo? * ¿Es preseleccionado el personal y los contratistas contratados en puestos sensibles? * ¿Se llevan a cabo controles de verificación del personal en el momento de solicitud de empleo? * Con los contratistas y los usuarios de tercera parte, ¿en el contrato se especifican claramente las responsabilidades de las partes y los procedimientos de notificación para su selección?
8.1.3	* ¿Se cuenta con acuerdos y cláusulas de confidencialidad adecuados? + ¿Se aceptan y firman los términos y condiciones laborales por parte de los empleados, contratistas y usuarios de tercera parte? + ¿Se establecen las obligaciones de las partes interesadas para la seguridad de información dentro de los términos y condiciones laborales?	* Revisar términos, condiciones, acuerdos y cláusulas laborales para empleados, contratistas y usuarios de tercera parte.	* ¿Se cuenta con acuerdos y cláusulas de confidencialidad adecuados? * ¿Se aceptan y firman los términos y condiciones laborales por parte de los empleados, contratistas y usuarios de tercera parte? * ¿Se establecen las obligaciones de las partes interesadas para la seguridad de información dentro de los términos y condiciones laborales?
8.2	* Revisar la conciencia, formación y los planes educativos de seguridad de la información. + ¿Los usuarios finales y la dirección reciben constantemente una formación adecuada en seguridad de la información, incluyendo los roles y responsabilidades, procedimientos de acceso (login), entre otros, en el contexto de capacitación general de los sistemas de TI?		

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
8.2.1	* ¿Se exige a empleados, contratistas y usuarios de terceras partes aplicar la seguridad de la información en concordancia con las políticas y los procedimientos establecidos por la organización? * ¿Los empleados, contratistas y usuarios de terceras partes tienen la concientización sobre seguridad de la información adecuado? * ¿Los empleados, contratistas y usuarios de terceras partes están de acuerdo con los términos y las condiciones laborales? * ¿Los empleados, contratistas y usuarios de terceras partes cuentan con las calificaciones y las habilidades apropiadas?	* Revisar compromisos asumidos por parte de los empleados, contratistas y usuarios de tercera parte con las políticas y procedimientos definidos para la seguridad de la información.	* ¿Se exige a empleados, contratistas y usuarios de terceras partes aplicar la seguridad de la información en concordancia con las políticas y los procedimientos establecidos por la organización? * ¿Los empleados, contratistas y usuarios de terceras partes tienen la concientización sobre seguridad de la información adecuado? * ¿Los empleados, contratistas y usuarios de terceras partes están de acuerdo con los términos y las condiciones laborales? * ¿Los empleados, contratistas y usuarios de terceras partes cuentan con las calificaciones y las habilidades apropiadas?
8.2.2	* ¿Los empleados, contratistas y usuarios de terceras partes reciben el entrenamiento o la formación apropiada en relación con las políticas y procedimientos organizacionales acordes con sus funciones laborales? * Así mismo, ¿reciben las actualizaciones regulares y pertinentes en relación con las políticas y procedimientos organizacionales acordes con sus funciones laborales?	* Revisar planes, programa y registros de formación, capacitación y concientización en seguridad de la información impartido a empleados, contratistas y usuarios de tercera parte de la empresa.	* ¿Los empleados, contratistas y usuarios de terceras partes reciben el entrenamiento o la formación apropiada en relación con las políticas y procedimientos organizacionales acordes con sus funciones laborales? * Así mismo, ¿reciben las actualizaciones regulares y pertinentes en relación con las políticas y procedimientos organizacionales acordes con sus funciones laborales?
8.2.3	* ¿Existe un proceso disciplinario formal para los empleados que han violado las políticas y procedimientos de seguridad de la organización? * ¿El proceso contempla realizar el retiro de las funciones, los derechos de acceso y los privilegios al empleado, contratista o usuario de tercera parte que presente un caso grave de mala conducta?	* Revisar documento con proceso disciplinario ante la violación de las políticas y procedimientos de seguridad de la información.	* ¿Existe un proceso disciplinario formal para los empleados que han violado las políticas y procedimientos de seguridad de la organización? * ¿El proceso contempla realizar el retiro de las funciones, los derechos de acceso y los privilegios al empleado, contratista o usuario de tercera parte que presente un caso grave de mala conducta?
8.3	Revisar las políticas, normas, procedimientos y directrices relativas a los elementos de seguridad de la información, como recuperación de activos de información, claves, eliminación de los derechos de accesos, entre otros.		

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
8.3.1	* Verificar que se definen y asignan claramente las responsabilidades dentro de la organización para ejecutar la finalización o cambio de un empleo. + ¿Se tienen en cuanta los requisitos de seguridad y las responsabilidades legales por un periodo de tiempo posterior a la terminación de la contratación laboral? + ¿Se incluyen en los contratos las responsabilidades y deberes válidos una vez terminen el contrato laboral los empleados, contratistas y usuarios de tercera parte? + ¿Los cambios de responsabilidades o del contrato laboral se gestiona como una terminación y se realiza un nuevo proceso de aceptación de términos y condiciones laborales?	Revisar documento donde se definen y asignan las responsabilidades de los empleados, contratistas o usuarios de tercera parte para ejecutar la finalización o cambio de empleo.	* Verificar que se definen y asignan claramente las responsabilidades dentro de la organización para ejecutar la finalización o cambio de un empleo. + ¿Se tienen en cuanta los requisitos de seguridad y las responsabilidades legales por un periodo de tiempo posterior a la terminación de la contratación laboral? + ¿Se incluyen en los contratos las responsabilidades y deberes válidos una vez terminen el contrato laboral los empleados, contratistas y usuarios de tercera parte? + ¿Los cambios de responsabilidades o del contrato laboral se gestiona como una terminación y se realiza un nuevo proceso de aceptación de términos y condiciones laborales?
8.3.2	* Verificar el procedimiento para la devolución de todos los activos en posesión de empleados, contratistas y terceros a la finalización de su empleo, contrato o acuerdo. + ¿Se cuenta con un proceso para la devolución de software, documentos corporativos, equipos y demás activos de la organización que se encuentre en su poder? + ¿Se cuenta con un procedimiento para asegurar que la información contenida en equipos o dispositivos de propiedad de los empleados, contratistas y usuarios de tercera parte se transfiera a la empresa y se elimine de manera segura de ese equipo? + ¿Se cuenta con un procedimiento para documentar y transferir el conocimiento de un empleado, contratista o usuario de tercera parte que se requiera para la continuidad de las operaciones de la empresa?	* Revisar política y procedimiento para la devolución de activos en posesión de empleados, contratistas y usuarios de tercera parte a la finalización de su empleo, contrato o acuerdo.	* Verificar el procedimiento para la devolución de todos los activos en posesión de empleados, contratistas y terceros a la finalización de su empleo, contrato o acuerdo. + ¿Se cuenta con un proceso para la devolución de software, documentos corporativos, equipos y demás activos de la organización que se encuentre en su poder? + ¿Se cuenta con un procedimiento para asegurar que la información contenida en equipos o dispositivos de propiedad de los empleados, contratistas y usuarios de tercera parte se transfiera a la empresa y se elimine de manera segura de ese equipo? + ¿Se cuenta con un procedimiento para documentar y transferir el conocimiento de un empleado, contratista o usuario de tercera parte que se requiera para la continuidad de las operaciones de la empresa?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
8.3.3	* Verificar que se retiran los derechos de acceso a todos los empleados, contratistas o usuarios de terceras partes a la información y a las instalaciones de procesamiento de información una vez terminado el empleo, contrato o acuerdo, o pasar por revisión en caso de cambio. + ¿Se cuenta con un proceso definido para el retiro de derechos de acceso a los activos asociados con los sistemas y servicios de información? + Cuando se realiza un cambio de cargo, ¿se retiran todos los accesos que no están aprobados para el cargo?	Revisar política y procedimiento para el retiro de derechos de acceso a todos los empleados, contratistas y usuarios de tercera parte a la información y a las instalaciones de procesamiento de información una vez terminado el empleo, contrato o acuerdo, o pasar por revisión en caso de cambio.	* Verificar que se retiran los derechos de acceso a todos los empleados, contratistas o usuarios de terceras partes a la información y a las instalaciones de procesamiento de información una vez terminado el empleo, contrato o acuerdo, o pasar por revisión en caso de cambio. + ¿Se cuenta con un proceso definido para el retiro de derechos de acceso a los activos asociados con los sistemas y servicios de información? + Cuando se realiza un cambio de cargo, ¿se retiran todos los accesos que no están aprobados para el cargo?
13			
13.1	* Revisar los procedimientos para la presentación de informes de eventos y debilidades de seguridad. * Trazar el proceso usando una muestra de documentación, como registros de Help Desk, comparando lo sucedido realmente con las políticas, procedimientos y directrices. * Confirmar quienes deben informar sobre los eventos y debilidades de seguridad son conscientes de, y en el uso real, el proceso.		
13.1.1	* ¿Existe un procedimiento formal para informar los eventos en la seguridad de información? * ¿Se tienen los canales de gestión apropiados para informarlos lo más pronto posible? * ¿Existe un procedimiento formal de escalada y respuesta oportuna y adecuada que contenga las acciones a seguir cuando se reporta un evento de seguridad de la información? * ¿Los empleados, contratistas y usuarios de tercera parte son conscientes de su responsabilidad para reportar los eventos de seguridad de la información cuando éstos sucedan?	* Revisar procedimiento para informar eventos en la seguridad de la información. * Revisar registros de eventos reportados en seguridad de la información.	* ¿Existe un procedimiento formal para informar los eventos en la seguridad de información? * ¿Se tienen los canales de gestión apropiados para informarlos lo más pronto posible? * ¿Existe un procedimiento formal de escalada y respuesta oportuna y adecuada que contenga las acciones a seguir cuando se reporta un evento de seguridad de la información? * ¿Los empleados, contratistas y usuarios de tercera parte son conscientes de su responsabilidad para reportar los eventos de seguridad de la información cuando éstos sucedan?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
13.1.2	* ¿Se exige a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información observar y reportar todas las debilidades encontradas relacionadas con la seguridad de los mismos? * ¿Existe un procedimiento formal de notificación dirigido a los usuarios para informar debilidades en la seguridad, o amenazas a los sistemas o servicios que brinda la empresa?	* Revisar procedimiento para informar debilidades en seguridad de la información. * Revisar registros de debilidades reportados en seguridad de la información	* ¿Se exige a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información observar y reportar todas las debilidades encontradas relacionadas con la seguridad de los mismos? * ¿Existe un procedimiento formal de notificación dirigido a los usuarios para informar debilidades en la seguridad, o amenazas a los sistemas o servicios que brinda la empresa?
13.2	* Revisar la evaluación o investigación, acción correctiva y las partes posteriores de los procesos para la gestión de incidentes de seguridad a oportunidades de mejora. * Comprobar los registros relativos a incidentes recientes para nuevas evidencias.		
13.2.1	* ¿Existe en la organización un proceso claro y formal para la gestión de incidentes de seguridad de la información? * ¿Se tienen definidas las responsabilidades y procedimientos adecuados para asegurar una respuesta rápida, efectiva y ordenada ante la presencia de un incidente de seguridad de información?	* Revisar procedimiento para la gestión de incidentes de seguridad de la información. * Revisar documento con asignación de responsabilidades en la gestión de incidentes de seguridad de la información.	* ¿Existe en la organización un proceso claro y formal para la gestión de incidentes de seguridad de la información? * ¿Se tienen definidas las responsabilidades y procedimientos adecuados para asegurar una respuesta rápida, efectiva y ordenada ante la presencia de un incidente de seguridad de información?
13.2.2	* ¿Existe un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes y fallos en la seguridad de información? * ¿Existe un aprendizaje proactivo sobre los incidentes, mejoras en el conocimiento de riesgos y los controles de seguridad de la información?	* Revisar procedimiento para monitorear y cuantificar los incidentes y fallos en seguridad de la información.	* ¿Existe un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes y fallos en la seguridad de información? * ¿Existe un aprendizaje proactivo sobre los incidentes, mejoras en el conocimiento de riesgos y los controles de seguridad de la información?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
13.2.3	* ¿Existe un procedimiento para recolectar, retener y presentar la evidencia de un incidente de seguridad de la información cuando una acción de seguimiento contra una persona u organización implica una acción legal? * ¿El proceso de recolección de los datos se ajusta a las prácticas jurídicas e industriales? * ¿El procedimiento es claro en proteger la integridad del material usado como evidencia durante el tratamiento del incidente?	* Revisar procedimiento para recolectar, retener y presentar evidencias de incidentes en seguridad de la información.	* ¿Existe un procedimiento para recolectar, retener y presentar la evidencia de un incidente de seguridad de la información cuando una acción de seguimiento contra una persona u organización implica una acción legal? * ¿El proceso de recolección de los datos se ajusta a las prácticas jurídicas e industriales? * ¿El procedimiento es claro en proteger la integridad del material usado como evidencia durante el tratamiento del incidente?
14			
14.1			

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
14.1.1	* ¿Existe un proceso gestión definido y mantenido para la continuidad del negocio en toda la organización? * ¿El personal involucrado en el proceso de gestión de incidentes tienen claras sus funciones y responsabilidades? * ¿Es adecuada la forma cómo la organización determina y satisface las necesidades de continuidad de negocio? * ¿Se comprende el impacto causado por los incidentes de seguridad de la información? * ¿Se tienen claros los objetivos del negocio para los servicios de procesamiento de información? * ¿Se tienen en cuenta las pólizas de seguro dentro del proceso de continuidad del negocio y de la gestión de riesgos operativos? * ¿El proceso incluye adicionar controles preventivos y de mitigación si es necesario? * ¿Existen en la empresa políticas, procedimientos, normas y directrices asociadas a la continuidad del negocio? * ¿Existe un plan de continuidad de negocio implantado por la empresa? * ¿Se cuanta con un plan de pruebas, revisiones y actualizaciones del proceso de continuidad del negocio? * ¿Existe evidencia de las pruebas regulares, las revisiones y las actualizaciones que se realizan en el proceso?	Revisar política y procedimiento de gestión de la continuidad del negocio en seguridad de la información de la organización.	* ¿Existe un proceso gestión definido y mantenido para la continuidad del negocio en toda la organización? + ¿Existe un plan de continuidad de negocio implantado por la empresa? + ¿Se cuanta con un plan de pruebas, revisiones y actualizaciones del proceso de continuidad del negocio? + ¿Existe evidencia de las pruebas regulares, las revisiones y las actualizaciones que se realizan en el proceso? ¿Existe en la organización un proceso claro y formal para la gestión de incidentes de seguridad de la i + ¿Se tienen claros los objetivos del negocio para los servicios de procesamiento de información? + ¿El proceso incluye adicionar controles preventivos y de mitigación si es necesario? + ¿Se tienen en cuenta las pólizas de seguro dentro del proceso de continuidad del negocio y de la gestión de riesgos operativos? * ¿Existen en la empresa políticas, procedimientos, normas y directrices asociadas a la continuidad del negocio? + ¿Es adecuada la forma cómo la organización determina y satisface las necesidades de continuidad de negocio? * ¿El personal involucrado en el proceso de gestión de incidentes tienen claras sus funciones y responsabilidades? + ¿Se comprende el impacto causado por los incidentes de seguridad de la información?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
14.1.2	* ¿El personal involucrado comprenden los riesgos a los que está enfrentada la organización? * ¿Se tienen identificados todos los procesos críticos y los activos asociados al negocio? * ¿Se identifican los impactos potenciales de los eventos que puedan causar interrupciones sobre los procesos críticos y activos del negocio? + ¿Se realiza una evaluación de riesgos adecuado para determinar el impacto de las interrupciones en la organización? + ¿Se ha desarrollado un plan estratégico en base a los resultados de la evaluación de riesgo para determinar un enfoque global de la continuidad del negocio?	* Revisar matriz de riesgo donde se identifiquen los riesgos asociados a la continuidad del negocio. * Revisar plan estratégico de la organización.	* ¿El personal involucrado comprenden los riesgos a los que está enfrentada la organización? * ¿Se tienen identificados todos los procesos críticos y los activos asociados al negocio? * ¿Se identifican los impactos potenciales de los eventos que puedan causar interrupciones sobre los procesos críticos y activos del negocio? + ¿Se realiza una evaluación de riesgos adecuado para determinar el impacto de las interrupciones en la organización? + ¿Se ha desarrollado un plan estratégico en base a los resultados de la evaluación de riesgo para determinar un enfoque global de la continuidad del negocio?
14.1.3	* ¿Se tiene un proceso de planificación de la continuidad de negocio adecuado? + ¿Se cuenta con un plan de continuidad del negocio adecuado y suficiente para satisfacer los requisitos de seguridad de la información de la empresa? * ¿Los diseños para garantizar la alta disponibilidad son empleados empleados adecuadamente para sistemas de TI, redes, entre otras, de apoyo a los procesos críticos del negocio? * ¿Los planes para restaurar las operaciones comerciales permiten la recuperación en el tiempo requerido después de una interrupción o falla de procesos de negocio? * ¿El plan de continuidad de negocio se pone a prueba y se actualiza regularmente?	Revisar plan de continuidad de negocio.	* ¿Se tiene un proceso de planificación de la continuidad de negocio adecuado? * ¿Se cuenta con un plan de continuidad del negocio adecuado y suficiente para satisfacer los requisitos de seguridad de la información de la empresa? * ¿Los diseños para garantizar la alta disponibilidad son empleados adecuadamente para sistemas de TI, redes, entre otras, de apoyo a los procesos críticos del negocio? * ¿Los planes para restaurar las operaciones comerciales permiten la recuperación en el tiempo requerido después de una interrupción o falla de procesos de negocio? * ¿El plan de continuidad de negocio se pone a prueba y se actualiza regularmente?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
14.1.4	* Verificar la existencia de una sola estructura para el plan de continuidad del negocio, asi como identificar las prioridades para pruebas y mantenimientos. + ¿Existe un único marco para el plan de continuidad del negocio? + ¿El marco es coherente para la planificación de la continuidad del negocio? + ¿Se mantiene este marco para asegurar que todos los planes sean coherentes y determinar las prioridades de prueba y mantenimiento? + ¿Se identifican las condiciones de activación y las personas responsables de la ejecución de cada componente del plan? * Verificar que todos los planes y consideraciones de los requisitos de la seguridad de la información son consistentes + ¿Los controles preventivos, predictivos y correctivos son adecuados? + ¿Las actividades de recuperación de desastres adoptadas por la empresa permiten la identificación y evaluación rápida de los acontecimientos que probablemente interrumpan los procesos de negocio? + ¿Los planes se han establecido adecuadamente para mantener las operaciones de negocios o restaurarlos en plazos definidos después de una interrupción o fallo? + ¿Los planes tienen en cuenta la identificación y acuerdo de responsabilidades, la identificación del procedimiento de recuperación y restauración, documentación de procedimientos y pruebas o ejercicios regulares?	Revisar plan de continuidad de negocio.	* Verificar la existencia de una sola estructura para el plan de continuidad del negocio, así como identificar las prioridades para pruebas y mantenimientos. + ¿Existe un único marco para el plan de continuidad del negocio? + ¿El marco es coherente para la planificación de la continuidad del negocio? + ¿Se mantiene este marco para asegurar que todos los planes sean coherentes y determinar las prioridades de prueba y mantenimiento? + ¿Se identifican las condiciones de activación y las personas responsables de la ejecución de cada componente del plan? * Verificar que todos los planes y consideraciones de los requisitos de la seguridad de la información son consistentes + ¿Los controles preventivos, predictivos y correctivos son adecuados? + ¿Las actividades de recuperación de desastres adoptadas por la empresa permiten la identificación y evaluación rápida de los acontecimientos que probablemente interrumpan los procesos de negocio? + ¿Los planes se han establecido adecuadamente para mantener las operaciones de negocios o restaurarlos en plazos definidos después de una interrupción o fallo? + ¿Los planes tienen en cuenta la identificación y acuerdo de responsabilidades, la identificación del procedimiento de recuperación y restauración, documentación de procedimientos y pruebas o ejercicios regulares?

Sigue en la página siguiente.

Anexo ISO 27001	Actividad general	Previo	En sitio
14.1.5	* ¿Se evalúan y prueban los planes de continuidad de negocio mediante el muestreo y la revisión de la documentación de procesos, informes, etc? * ¿El marco asegura que todos los planes son coherentes e identifican las prioridades para realizar pruebas y mantenimientos? * ¿Se realizan pruebas y revisiones periódicas y programadas con anterioridad de los planes de continuidad del negocio para garantizar que están siendo actualizados y son eficaces el la práctica? * ¿El programa de gestión de cambios de la organización asegura que los procedimientos incluyan aspectos de continuidad de negocio para un tratamiento adecuado?	* Revisar cronograma de pruebas de planes de continuidad de negocio de la organización. * Revisar informes de pruebas de planes de continuidad de negocio realizados en la organización. * Revisar procedimiento de control de cambios.	? ¿Se evalúan y prueban los planes de continuidad de negocio mediante el muestreo y la revisión de la documentación de procesos, informes, etc? * ¿El marco asegura que todos los planes son coherentes e identifican las prioridades para realizar pruebas y mantenimientos? * ¿Se realizan pruebas y revisiones periódicas y programadas con anterioridad de los planes de continuidad del negocio para garantizar que están siendo actualizados y son eficaces el la práctica? * ¿El programa de gestión de cambios de la organización asegura que los procedimientos incluyan aspectos de continuidad de negocio para un tratamiento adecuado?

Fuente: *Autor*

La tabla anterior permitió modelar los procesos de auditoría interna propuestos en este proyecto y que se explicarán en el siguiente apartado.

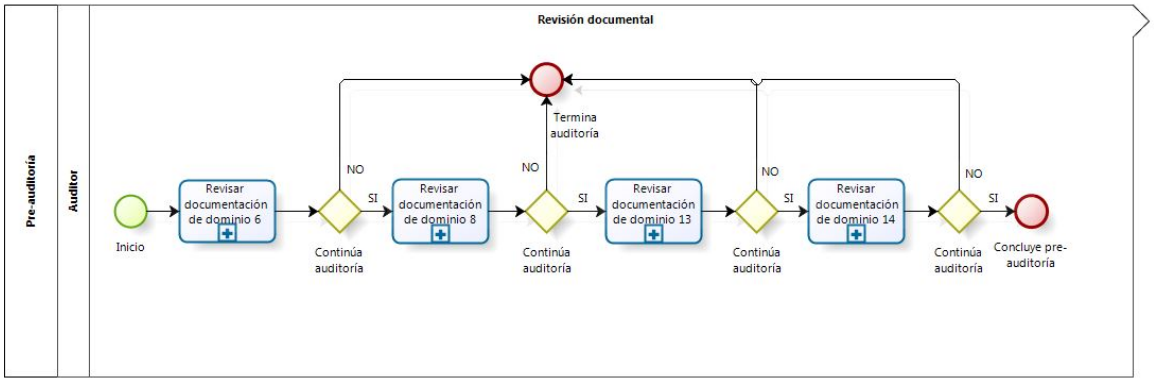
7.2. PROCESOS DE AUDITORÍA INTERNA

El proceso de auditoría propuesto, se estructura en dos procesos macro:

- **Pre-auditoría:** En este proceso se revisa la documentación y los requisitos de cumplimiento que el auditor le solicita a la empresa antes de realizar la auditoría en el sitio.
- **En sitio:** En este proceso se revisa el cumplimiento de cada uno de los controles incluidos en cada dominio.

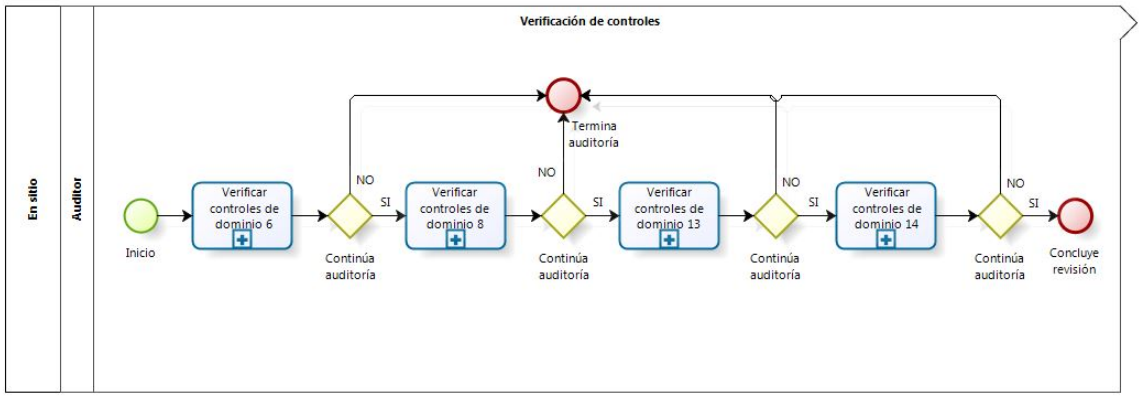
A continuación se muestra el modelo del proceso de auditoría interna definido para cada uno de los procesos macro establecidos:

Figura 7.1: *Proceso de pre-auditoría.*



Fuente: Autor

Figura 7.2: *Proceso de auditoría en sitio.*



Fuente: Autor

7.3. PROCESOS MACRO DE PRE-AUDITORÍA.

En este apartado se definen cada uno de los procesos previos realizados en una pre-auditoría para los aspectos *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"*.

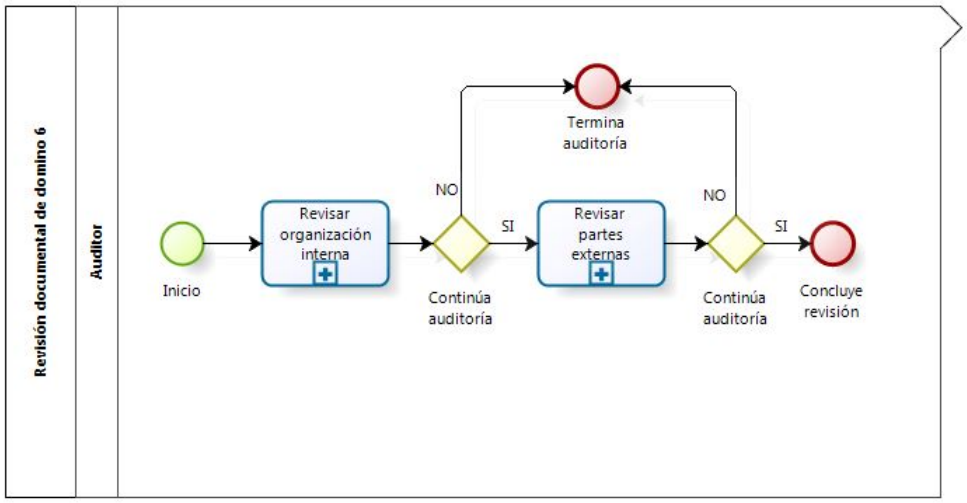
7.3.1. Organización de la seguridad de la información.

Tabla 7.4: ***Organización de la seguridad de la información***

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Procedimientos y controles que apoyan el SGSI.* ■ *Informe resultante de la evaluación del riesgo.* ■ *Plan de tratamiento de riesgos.* ■ *Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.* ■ *Registros.* ■ *Declaración de aplicabilidad.* ■ *Procedimiento de gestión de toda la documentación del SGSI.*
OBJETIVOS DEL PROCESO:
Revisar la documentación que soporta la gestión de la seguridad de la información dentro de la organización.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los dos subprocesos que la respaldan: ■ *Revisión de la documentación asociada a la organización interna.* ■ *Revisión de la documentación asociada a las partes externas.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):
Auditor interno.
PARTICIPANTES:
No aplica.
PROCESOS DE SOPORTE ASOCIADOS:

- *Revisar organización interna.*
- *Revisar partes externas.*

DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:

- *Documento de no conformidades*
- *Informe parcial de auditoría*

OBSERVACIONES:

Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

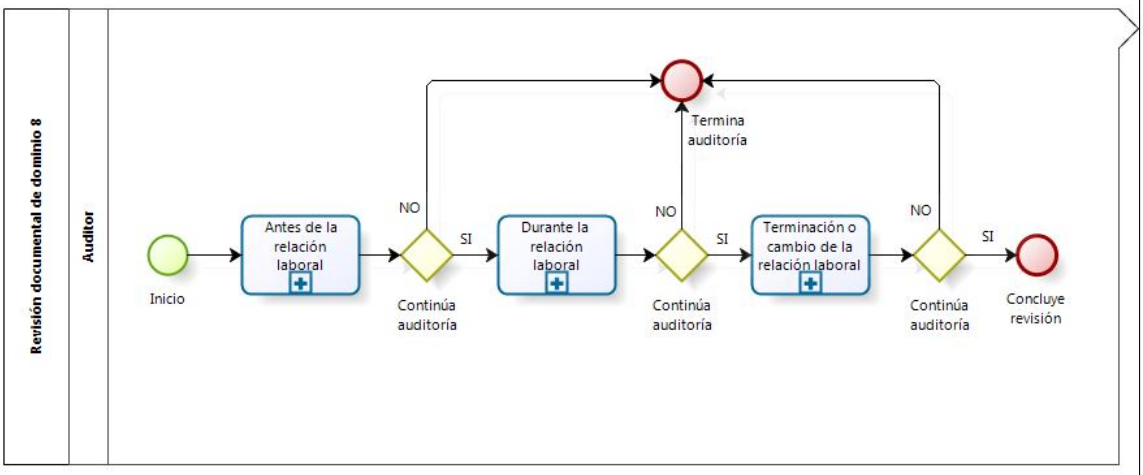
Fuente: *Autor*

7.3.2. Seguridad de los recursos humanos.

Tabla 7.5: ***Seguridad de los recursos humanos.***

SEGURIDAD DE LOS RECURSOS HUMANOS
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Procedimientos y controles que apoyan el SGSI.* ■ *Informe resultante de la evaluación del riesgo.* ■ *Plan de tratamiento de riesgos.* ■ *Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.* ■ *Registros.* ■ *Declaración de aplicabilidad.* ■ *Procedimiento de gestión de toda la documentación del SGSI.*
OBJETIVOS DEL PROCESO:
Revisar la documentación asociada a la gestión del recurso humano de la organización en cuanto a la seguridad de la información.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los tres subprocesos que la respaldan: ■ *Antes de la relación laboral.* ■ *Durante la relación laboral.* ■ *Terminación o cambio de la relación laboral.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):

Auditor interno.
PARTICIPANTES:
No aplica.
PROCESOS DE SOPORTE ASOCIADOS:
■ *Antes de la relación laboral* ■ *Durante la relación laboral.* ■ *Terminación o cambio de la relación laboral.*
DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:
■ *Documento de no conformidades* ■ *Informe parcial de auditoría*
OBSERVACIONES:
Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

7.3.3. Gestión de los incidentes de seguridad de la información.

Tabla 7.6: ***Gestión de los incidentes de seguridad de la información.***

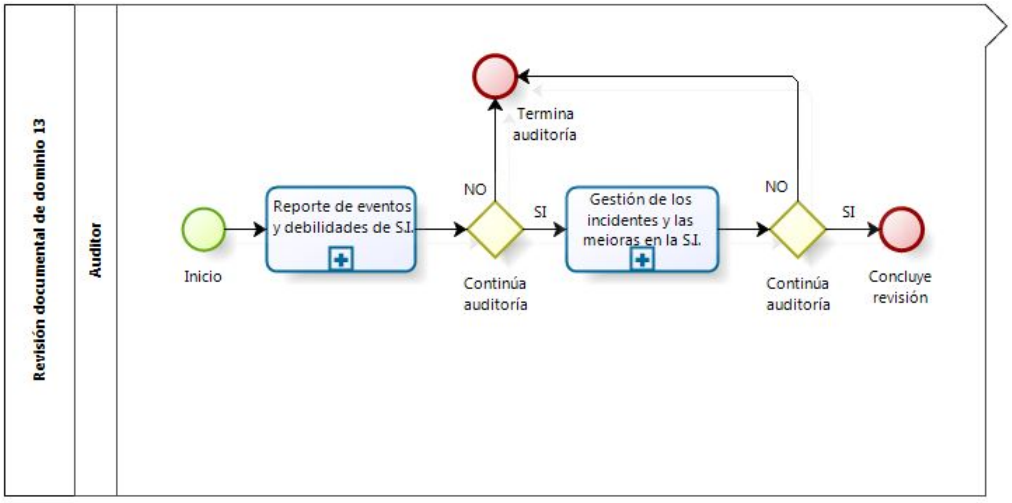
GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Procedimientos y controles que apoyan el SGSI.* ■ *Informe resultante de la evaluación del riesgo.* ■ *Plan de tratamiento de riesgos.* ■ *Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.* ■ *Registros.* ■ *Declaración de aplicabilidad.* ■ *Procedimiento de gestión de toda la documentación del SGSI.*
OBJETIVOS DEL PROCESO:
Revisar la documentación asociada a la gestión de los incidentes de seguridad de la información en la organización.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los dos subprocesos que la respaldan: ■ *Reporte de eventos y debilidades de seguridad de la información.* ■ *Gestión de los incidentes y las mejoras en la seguridad de la información.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):
Auditor interno.
PARTICIPANTES:

No aplica.

PROCESOS DE SOPORTE ASOCIADOS:

- *Reporte de eventos y debilidades de seguridad de la información.*
- *Gestión de los incidentes y las mejoras en la seguridad de la información.*

DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:

- *Documento de no conformidades*
- *Informe parcial de auditoría*

OBSERVACIONES:

Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

7.3.4. Gestión de la continuidad del negocio.

Tabla 7.7: ***Gestión de la continuidad del negocio.***

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Procedimientos y controles que apoyan el SGSI.* ■ *Informe resultante de la evaluación del riesgo.* ■ *Plan de tratamiento de riesgos.* ■ *Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.* ■ *Registros.* ■ *Declaración de aplicabilidad.* ■ *Procedimiento de gestión de toda la documentación del SGSI.*
OBJETIVOS DEL PROCESO:
Revisar la documentación asociada a la gestión de continuidad del negocio.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Este proceso consta de las siguiente actividades:

- *Revisar política y procedimiento de gestión de la continuidad del negocio en seguridad de la información de la organización.*
- *Gestión de los incidentes y las mejoras en la seguridad de la información.*
- *Revisar matriz de riesgo donde se identifiquen los riesgos asociados a la continuidad del negocio.*
- *Revisar plan estratégico de la organización.*
- *Revisar plan de continuidad de negocio.*
- *Revisar cronograma de pruebas de planes de continuidad de negocio de la organización.*
- *Revisar informes de pruebas de planes de continuidad de negocio realizados en la organización.*
- *Revisar procedimiento de control de cambios.*

Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.
Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.

RESPONSABLE(S):
Auditor interno.
PARTICIPANTES:
No aplica.
PROCESOS DE SOPORTE ASOCIADOS:
No tiene.
DIAGRAMA DEL PROCESO:
Ver Figura A.1 en el Apendice A
SALIDA DEL PROCESO:

- *Documento de no conformidades*
- *Informe parcial de auditoría*

OBSERVACIONES:
Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

7.4. PROCESOS MACRO DE AUDITORÍA EN SITIO.

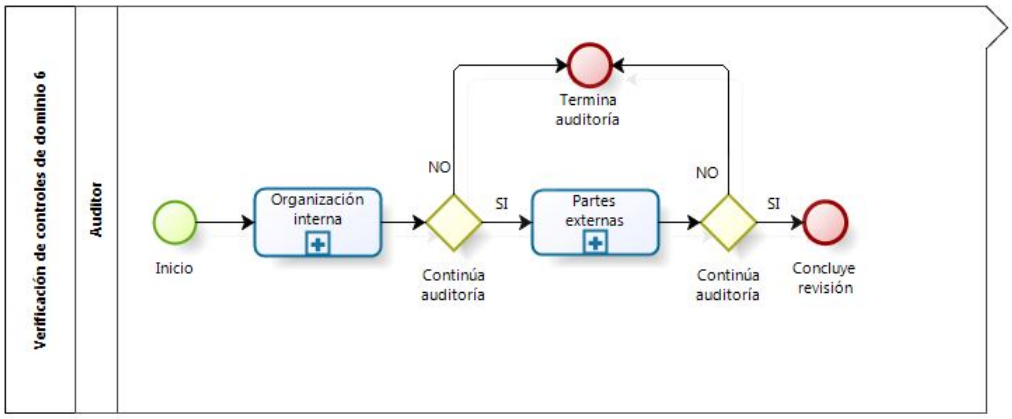
En este apartado se definen cada uno de los procesos realizados en una auditoría en sitio para los aspectos *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de incidentes de seguridad de la información"* y *"Gestión de la continuidad de negocio"*.

7.4.1. Organización de la seguridad de la información.

Tabla 7.8: ***Organización de la seguridad de la información***

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
▪ *Política y objetivos de seguridad.* ▪ *Alcance del SGSI.* ▪ *Declaración de aplicabilidad.* ▪ *Plan de auditoría.* ▪ *Lista de verificación.*
OBJETIVOS DEL PROCESO:
Verificar la correcta organización de la seguridad de la información en la organización.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los dos subprocesos que la respaldan: ▪ *Verificar controles asociados a la organización interna.* ▪ *Verificar controles asociados a las partes externas.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):
Auditor interno.

PARTICIPANTES:
Gerente, líder de cada área de la empresa donde se implemente el SGSI y coordinador del comité de seguridad de la información.
PROCESOS DE SOPORTE ASOCIADOS:
▪ *Organización interna.* ▪ *Partes externas.*
DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:
▪ *Documento de no conformidades* ▪ *Informe parcial de auditoría*
OBSERVACIONES:
Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

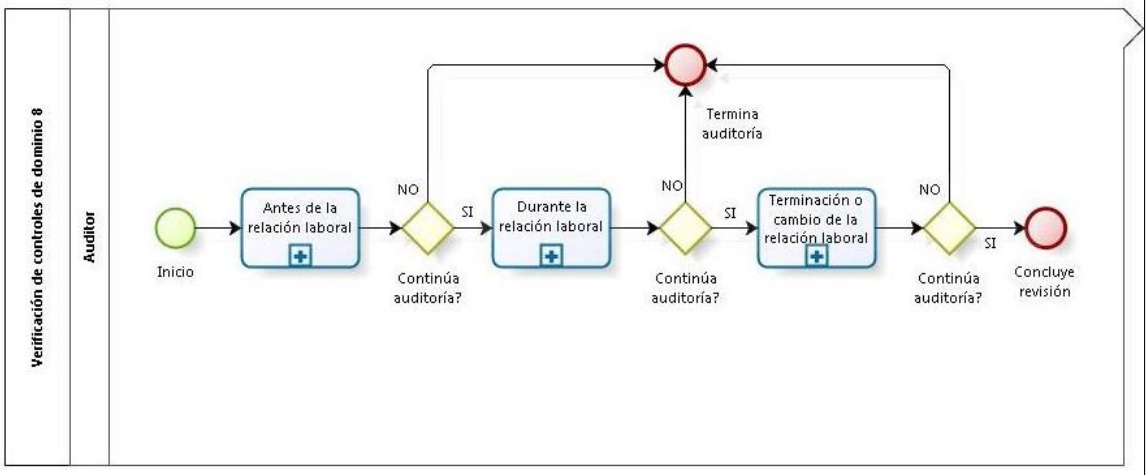
7.4.2. Seguridad de los recursos humanos.

Tabla 7.9: ***Seguridad de los recursos humanos.***

SEGURIDAD DE LOS RECURSOS HUMANOS
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
▪ *Política y objetivos de seguridad.* ▪ *Alcance del SGSI.* ▪ *Declaración de aplicabilidad.* ▪ *Plan de auditoría.* ▪ *Lista de verificación.*
OBJETIVOS DEL PROCESO:
Verificar que se cumplen con los controles asociados al antes, el durante y el después o cambio de la relación laboral con empleados, contratistas y usuarios de tercera parte.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los tres subprocesos que la respaldan: ▪ *Verificar los controles asociados al proceso previo a la relación laboral.* ▪ *Verificar los controles asociados al proceso del durante la relación laboral.* ▪ *Verificar los controles asociados al proceso de terminación o cambio de la relación laboral.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):
Auditor interno.
PARTICIPANTES:
Gerente, líder de cada área de la empresa donde se implemente el SGSI y coordinador del comité de seguridad de la información.
PROCESOS DE SOPORTE ASOCIADOS:

- *Antes de la relación laboral en sitio*
- *Durante la relación laboral en sitio.*
- *Terminación o cambio de la relación laboral en sitio.*

DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:

- *Documento de no conformidades*
- *Informe parcial de auditoría*

OBSERVACIONES:

Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

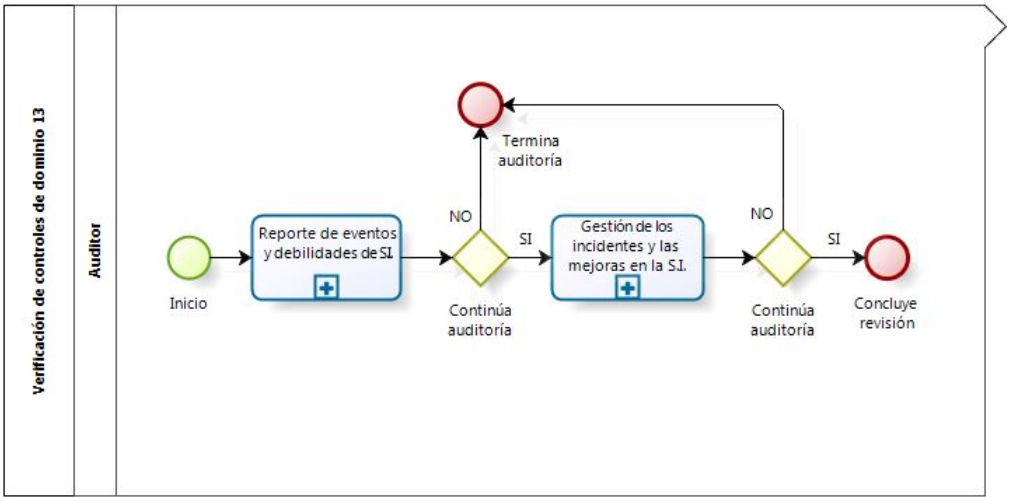
7.4.3. Gestión de los incidentes de seguridad de la información.

Tabla 7.10: ***Gestión de los incidentes de seguridad de la información.***

GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Declaración de aplicabilidad.* ■ *Plan de auditoría.* ■ *Lista de verificación.*
OBJETIVOS DEL PROCESO:
Verificar el cumplimiento de los controles asociados a la gestión de los incidentes de seguridad de la información.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los dos subprocesos que la respaldan: ■ *Verificar los controles asociados al reporte de eventos y debilidades de seguridad de la información.* ■ *Verificar los controles asociados a la gestión de los incidentes y las mejoras en la seguridad de la información.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):
Auditor interno.
PARTICIPANTES:
Gerente, líder de cada área de la empresa donde se implemente el SGSI y coordinador del comité de seguridad de la información.
PROCESOS DE SOPORTE ASOCIADOS:

- *Reporte de eventos y debilidades de seguridad de la información en sitio.*
- *Gestión de los incidentes y las mejoras en la seguridad de la información en sitio.*

DIAGRAMA DEL PROCESO:



Fuente: Autor

SALIDA DEL PROCESO:

- *Documento de no conformidades*
- *Informe parcial de auditoría*

OBSERVACIONES:

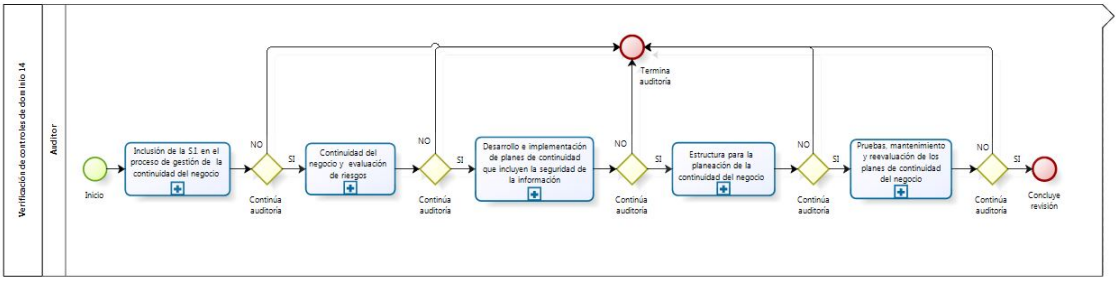
Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

7.4.4. Gestión de la continuidad del negocio.

Tabla 7.11: ***Gestión de la continuidad del negocio.***

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
TIPO DE PROCESO:
Proceso principal
ENTRADAS DEL PROCESO:
■ *Política y objetivos de seguridad.* ■ *Alcance del SGSI.* ■ *Declaración de aplicabilidad.* ■ *Plan de auditoría.* ■ *Lista de verificación.*
OBJETIVOS DEL PROCESO:
Verificar que se contrarrestan las interrupciones en las actividades del negocio y protegen sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y aseguran su recuperación oportuna.
DESCRIPCIÓN DEL PROCESO Y ACTIVIDADES:
Para el desarrollo del proceso, deben cumplirse con las actividades propuestas en los cinco subprocesos que la respaldan: ■ *Verificar los controles asociados a la inclusión de la Seguridad de la Información en el proceso de gestión de la continuidad del negocio.* ■ *Verificar los controles asociados a la continuidad del negocio y la evaluación de riesgos.* ■ *Verificar los controles asociados al desarrollo e implementación de planes de continuidad que incluyen seguridad de la información.* ■ *Verificar los controles asociados a la estructura para la planeación de la continuidad del negocio.* ■ *Verificar los controles asociados a pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.* *Si estas actividades se cumplen, se deja registro por escrito donde se indique la conformidad; si el auditor considera necesario hacer una observación, también debe registrarse por escrito.* *Si algunas de las actividades anteriores no se cumplen, debe declararse una no conformidad, mayor o menor, según las consideraciones del auditor interno, dejando la observación correspondiente al proceso para ser tenidas en cuenta en el informe de auditoría.*
RESPONSABLE(S):

Auditor interno.
PARTICIPANTES:
Gerente, líder de cada área de la empresa donde se implemente el SGSI y coordinador del comité de seguridad de la información.
PROCESOS DE SOPORTE ASOCIADOS:
■ Inclusión de la S.I. en el proceso de gestión de la continuidad del negocio. ■ *Continuidad del negocio y evaluación de riesgos.* ■ *Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información.* ■ *Estructura para la planeación de la continuidad del negocio.* ■ *Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.*
DIAGRAMA DEL PROCESO:
 **Fuente:** Autor
SALIDA DEL PROCESO:
■ *Documento de no conformidades* ■ *Informe parcial de auditoría*
OBSERVACIONES:
Para la ejecución de este proceso deben tenerse disponibles los documentos de entrada del proceso y otros documentos de soporte y/o herramientas que el auditor considere necesarias para validar el proceso.

Fuente: *Autor*

PROCESO DE AUDITORÍA INTERNA EN PRUEBA PILOTO

Con el fin de validar el modelo de auditoría interna propuesto, se realiza una prueba de auditoría en una empresa de la región. El objetivo de esta auditoría es poner en evidencia el estesdo actual de la empresa frente a la seguridad de la infrmación y de paso medir la pertinencia de los medelos desarrollados para los aspectos de *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de los incidentes de seguridad de la información"* y *"Gestión de la continuidad del negocio"* en una auditoría real.

La prueba se divide en dos momentos: en primera instancia se realiza la pre-auditoría y finalmente la auditoría en sitio. Para cada uno de los momentos, se cuentan con las herramientas anexas en el Apéndice B.

8.1. PRE-AUDITORÍA

Antes de iniciar con la pre-auditoría, es necesario contextualizar a los facilitares de la prueba piloto. En este primer acercamiento con la empresa, se realiza una breve descripción del proyecto de grado, el objetivo de la auditoría en los aspectos estudiados y los resultados que se esperan una vez concluido el proceso de auditoría en sitio. Así mismo, fue necesario formalizar la actividad mediante un acuerdo de confidencialidad firmado entre la empresa y el Grupo de Investigación en Telecomunicaciones NYQUIST.

8.1.1. Preparación de la pre-auditoría

La pre-auditoría consiste en realizar una revisión general de las políticas, porcedimientos y procesos que se llevan acabo en la empresa y están incluidos dentro del alcance de los controles de los aspectos a auditar. En esta primera etapa, se envío un oficio solicitando la siguiente información a la empresa:

Tabla 8.1: ***Documentación requerida por dominios***

Documentación propia del dominio	Documentación general para el SGSI
Organización de la seguridad de la información (dominio 6)	
Asignación de funciones y responsabilidades para coordinar y revisar el SGSI.	Estructura organizacional para la gestión del SGSI dentro de la organización.
Acta formal con asignación del director de seguridad de la información aprobada por la dirección.	Declaración de aplicabilidad.
Acuerdos con grupos de interés especiales en seguridad de la información.	Documento de aprobación de alcance y límites del SGSI.
Acuerdos de confidencialidad entre la empresa y sus clientes.	Informes de auditorías previas.
Acuerdos de responsabilidades y confidencialidad con terceras partes.	Informes de revisión de políticas.
Acuerdos o contratos con partes externas.	Informes de revisión independiente en seguridad de la información.
Clausulas o acuerdos de confidencialidad con partes externas.	Inventario de activos.
Clausulas o acuerdos definido para contratos con empleados, contratistas y terceras partes en relación acceso a activos críticos de la organización.	Matriz de riesgos de seguridad de la información.
Documento con la clasificación de la información.	Metodología de gestión de riesgos aprobada.
Inventario de activos administrados por partes externas.	Política de seguridad de la información.
Inventario de activos con información confidencial.	
Niveles de acceso a la información, sistemas de procesamiento de información y/o instalaciones.	
Plan de continuidad de negocio.	
Planes de educación, formación y concientización en seguridad de la información.	
Política de control de acceso.	
Procedimiento para asignar niveles de autorización.	
Procedimiento para autorización para los servicios de procesamiento de información.	
Procedimiento para control de cambios y actualizaciones.	
Procedimiento para gestión de acceso a partes externas a la información y/o a los -sistemas de procesamiento de información.	
Procedimiento para la devolución o destrucción de información confidencial.	
Requisitos para conceder acceso a los clientes (procedimiento).	
Requisitos para proteger la información confidencial usando términos que se puedan hacer -cumplir legalmente.	
Segregación de funciones.	
Seguridad de los recursos humanos (dominio 8)	
Acuerdo de aceptación de políticas, términos y condiciones en relación con la seguridad de la información.	Política de seguridad de la información.

Sigue en la página siguiente.

Documentación propia del dominio	Documentación general para el SGSI
Acuerdo de confidencialidad según las funciones y responsabilidades de seguridad del cargo.	Inventario de activos.
Clausula o acuerdo de confidencialidad en seguridad de la información.	Declaración de aplicabilidad.
Formato de contrato laboral con empleados, contratistas y usuarios de tercera parte.	Roles y responsabilidades en cuanto a seguridad de la información.
Informes de violaciones a la seguridad.	
Lista de verificación de hojas de vida de candidatos.	
Manual de funciones de cargos.	
Niveles de acceso.	
Planes de formación, educación y concientización en seguridad de la información y uso adecuado de los servicios de procesamiento de información.	
Procedimiento de evaluación laboral de los cargos.	
Procedimiento de inducción en seguridad de la información.	
Procedimiento para el cambio de responsabilidades y relaciones laborales dentro de la organización.	
Procedimiento para el retiro de derechos de acceso.	
Procedimiento para la devolución de activos.	
Procedimiento para la elección de personal (empleados, contratistas y usuarios de tercera parte).	
Procedimiento para la gestión de retiro de empleados, contratistas y usuarios de tercera parte.	
Proceso disciplinario formal para el manejo de violaciones de la seguridad.	
Programa de capacitación, educación y concientización en seguridad de la información.	
Programa de incentivos.	
Registros de capacitación, concientización y educación en seguridad.	
Responsabilidades del empleado, contratistas y usuarios de tercera parte en relación con la seguridad de la información.	
Roles y responsabilidades de cada cargo de la empresa.	
Gestión de los incidentes de la seguridad de la información (dominio 13)	
Formato y registro de reportes de incidentes de seguridad.	Matriz de riesgos de seguridad de la información.
Formato y registro de seguimiento a incidentes reportados.	Política de seguridad de la información.
Formato y reporte de evaluación de incidentes de seguridad.	Registros de auditorías previas.
Procedimiento de escalada y respuesta para atender eventos de seguridad.	
Procedimiento para recolección y presentación de evidencia.	
Procedimiento para reporte de incidentes de seguridad.	
Gestión de la continuidad del negocio (dominio 14)	
Plan de continuidad de negocio.	Política de seguridad de la información.

Sigue en la página siguiente.

Documentación propia del dominio	Documentación general para el SGSI
Procedimiento de recuperación y restauración de las operaciones de negocio.	Declaración de aplicabilidad.
Procedimientos de apoyo al plan de continuidad de negocio.	Matriz de riesgos.
Cronograma de pruebas y revisiones del plan de continuidad del negocio.	Inventario de activos.
Funciones y responsabilidades en plan de continuidad de negocio.	
Programa de educación, capacitación y concientización sobre el plan de continuidad de negocio.	
Acuerdos con proveedores.	
Registros e informes de pruebas y revisiones del plan de continuidad de negocio.	

Fuente: *Autor*

La información solicitada cumple con dos (2) objetivos:

- Conocer el grado actual de cumplimiento en seguridad de la información de la empresa.
- Determinar el alcance real de la auditoría en sitio.

La revisión documental permitió identificar cuales controles aplicaban en la empresa y cuales no, lo que permitió definir el punto de partida de la auditoría en sitio y establecer la ruta de trabajo durante la verificación de la eficiencia de los controles implementados. Así mismo, se identificaron las debilidades actuales de la empresa en el cumplimiento de la seguridad de la información. Cabe aclarar, que la empresa actualmente cuenta con buenas prácticas en seguridad de la información, pero no cuenta con un SGSI implementado. La prueba piloto permitirá a la empresa mejorar sus procesos actuales e identificar los requisitos de seguridad ausentes en el actual modelo de seguridad propuesto por ella.

8.1.2. Ejecución de la pre-auditoría

Durante la pre-auditoría se realizaron las actividades tendientes a validar la existencia de la documentación general de un SGSI y la necesaria para evaluar cada uno de los controles de los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006. Una vez concluida la revisión documental, se genera un informe parcial de pre-auditoría, el cual es socializado y puesto en aprobación por parte de la empresa; el documento no presenta observaciones, recomendaciones o solicitud de ajustes en la socialización con los facilitadores.

8.1.2.1. Criterios de evalaución

Los criterios tenidos en cuenta para la pre-auditoría fueron los siguientes:

- **Cumple:** Se verifica si la empresa cumple con el requisito de la norma. Las opciones asociadas son **Si** para cumple con el requisito relacionado y **No** en caso contrario.
- **No conformidad:** Si se presenta un incumplimiento, se evalua si debe considerarse una no conformidad o no. Las opciones son **Si** en caso de considerar no conformidad respecto al incumplimiento y **No** en caso contrario.
- **Tipo de no conformidad** Se establece el tipo de no conformidad según el criterio del auditor. Las opciones asociadas son **Mayor**, **menor** y **Observación**.
- **No aplica:** Permite identificar aquellos incumplimientos para los cuales la empresa no tiene implementado controles o no es exigencia para el desarrollo de sus procesos.
- **Observaciones:** En esta casilla se describe la razón por la cual se determina o no la no conformidad, así como las anotaciones que el auditor considere necesarios.

8.1.2.2. Tiempo de pre-auditoría

Se estimó un tiempo para realizar la revisión documental de 4 horas, siguiendo el siguiente orden:

- Documentación general del SGSI : 40 minutos.
- Organización de la seguridad de la información : 1 hora.
- Seguridad de los recursos humanos : 1 hora.
- Gestión de los incidentes de seguridad de la información : 40 minutos.
- Gestión de la continuidad del negocio : 40 minutos.

8.1.3. Resultado de la pre-auditoría

Las actividades desarrolladas durante esta etapa, corresponden a realizar la revisión de la documentación enviada por la empresa. Tal y como se estableció en el apartado anterior, se inicia por la revisión de la documentación general hasta el proceso de gestión de continuidad del negocio. Para la ejecución de esta etapa se tiene como base los formatos *"Lista de chequeo docucumentacion.xlsx"*, el cual contiene el listado de la documentación solicitada a la empresa,

y *"Preauditoria.xlsx"*, que contiene la lista de verificación por dominio. Al final de la actividad, se genera un documento con el informe parcial de pre-auditoría, el cual es socializado con la empresa para su validación y aprobación. Sin esta aprovación, no es posible generar el plan de auditoría en sitio.

En el Apéndice C, puede apreciarse el informe parcial de la pre-auditoría.

8.2. AUDITORÍA EN SITIO

La auditoría en sitio es la última etapa del modelo planteado en este proyecto. Consiste en hacer la comprobación en sitio de los controles, procedimientos y planes identificados durante la revisión documental y consignado en el informe parcial de pre-auditoría. El objetivo es corraborar que la empresa cumple con lo establecido en su política de seguridad y demás documentos de soporte al SGSI. Sin embargo, la empresa donde se realizó la prueba piloto no cuenta con un SGSI definido, pero si aplican buenas prácticas de seguridad de la información. Partiendo de la propuesta de seguridad planteada por la empresa, se genera un plan de auditoría en sitio.

8.2.1. Plan de auditoría

El plan de auditoría se presenta a la empresa mediante oficio para su aprobación. Es necesario que la empresa esté de acuerdo con el plan de auditoría para programar la fecha y hora de la prueba, así como notificar al personal que hará parte del ejercicio. El plan de auditoría propuesto se presenta a continuación:

1. ***OBJETIVO DE LA AUDITORÍA***
   Verificar que la empresa cumple con los requisitos asociados a los controles de los dominios de control 6 "Organización de la seguridad de la informació", 8 "Gestión del recurso humano", 13 "Gestión de incidentes de seguridad de la información" y 14 "Gestión de la continuidad del negocio" de la norma NTC-ISO/IEC 27001:2006.

2. ***ALCANCE***
   El alcance está determinado por los procesos cubiertos por los controles de los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006.

3. ***ÁREA(S) AUDITABLES***
   Las áreas incluidas en el proceso de auditoria comprenden:

   - *Gerencia.*
   - *Seguridad.*
   - *Demás áreas involucradas en los proceso objeto de auditoria.*

4. ***PERSONAS AUDITABLES***
   Las personas incluidas en el proceso de auditoria se relacionan a continuación:

   - *Gerente.*

- *Líder de seguridad.*
- *Personal de apoyo a los procesos incluidos en el proceso de auditoría.*

5. ***PROCESO DE AUDITORIA EN SEGURIDAD DE LA INFORMACIÓN***
La siguiente tabla establece el orden procesos a auditar y los tiempos de ejecución de la auditoria de cada uno de ellos:

Tabla 8.2: ***Tiempo de procesos a auditar***

Orden	***Proceso auditable***	***Actividades a desarrollar***	***Tiempo estimado (Horas)***
1	*Gerencia general*	*Verificar conformidad de la documentación general.*	*1*
		Verificar la gestión recurso humano.	*2*
2	*Seguridad*	*Verificar la conformidad de la organización de la seguridad de la información.*	*1,5*
		Verificar la gestión de incidentes de seguridad.	*1*
		Verificar el cumplimiento de los planes de continuidad de negocio (estrategias)	*2*
Tiempo total de auditoría			*7,5*

Fuente: *Autor*

6. ***DOCUMENTOS CONSULTADOS***
Los siguientes son los documentos entregados por la empresa para realizar el análisis inicial del proceso de auditoria:

- *INVENTARIOS-actualizado.xls.*
- *LISTADO_PROPIEDAD_INTELECTUAL.doc.*
- *LISTADO_PROPIETARIO.docx.*
- *MAPA_TOPOLOGICO_DE_LA_RED.doc.*
- *ORGANIGRAMA.docx.*
- *PERSONAS_AUTORIZADAS_A_MANIPULACION_DE_INFORMACION.docx.*
- *POLITICAS DE SEGURIDAD.doc.*
- *REGISTRO_FORMAL_DE_USUARIOS.docx.*
- *RESPONSABLE_ACTIVO_SIN_ASIGNAR.docx.*

7. ***OBSERVACIONES***

- *El plan de auditoria propuesto está sujeto a los cambios que la empresa considere necesarios para llevar a cabo el proceso de auditoria en sitio.*
- *El objetivo de la auditoria es dar a conocer el estado real de los controles actualmente implementados e identificar los puntos críticos que requieren atención inmediata o están tendientes a oportunidades de mejora.*

8.2.2. Criterios de evalaución

Los criterios tenidos en cuenta para la auditoría en sitio fueron los siguientes:

- **Cumple:** Se verifica si la empresa cumple con el requisito de la norma. Las opciones asociadas son **Si** para cumple con el requisito relacionado y **No** en caso contrario.
- **No conformidad:** Si se presenta un incumplimiento, se evalua si debe considerarse una no conformidad o no. Las opciones son **Si** en caso de considerar no conformidad respecto al incumplimiento y **No** en caso contrario.
- **Tipo de no conformidad** Se establece el tipo de no conformidad según el criterio del auditor. Las opciones asociadas son **Mayor**, **menor** y **Observación**.
- **No aplica:** Permite identificar aquellos incumplimientos para los cuales la empresa no tiene implementado controles o no es exigencia para el desarrollo de sus procesos.
- **Observaciones:** En esta casilla se describe la razón por la cual se determina o no la no conformidad, así como las anotaciones que el auditor considere necesarios.

8.2.3. Lista de verificación

A partir del modelo propuesto, se genera una lista de chequeo para validar el cumplimiento de los controles asociados a los aspectos *"Organización de la seguridad de la información"*, *"Seguridad de los recursos humanos"*, *"Gestión de los incidentes de seguridad de la información"* y *"Gestión de la continuidad del negocio"*. La herramienta de evaluación puede apreciarse en el Apéndice B.

ARQUITECTURA DEL MODELO

Como propuesta para automatizar el modelo presentado en el apartado 7, se presenta una arquitectura basada en *Spring Framework*, *Java* e *Hibernate*. En la figura 9.1 se aprecia la arquitectura general para una automatización de una herramienta orientada a la Web para auditar los controles de los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006.

9.1. DESCRIPCIÓN DE COMPONENTES

9.1.1. Interfaz de usuario

Permite la comunicación del usuario final con la aplicación Web. Por tratarse de una herramienta orientada a la Web, las solicitudes se realizarán mediante el protocolo HTTP.

9.1.2. Spring MVC

Basado en la arquitectura *MVC* (por sus siglas en ingles *Model-View-Controller*). El *modelo-vista-controlador* es un paradigma de programación que propone separar el código de los programas. Es una propuesta de diseño de software para la implementación de interfaces de usuarios en sistemas donde sea requerido. Se fundamenta en la separación de código en tres capas diferentes, denominadas modelos, vistas y controladores[1].

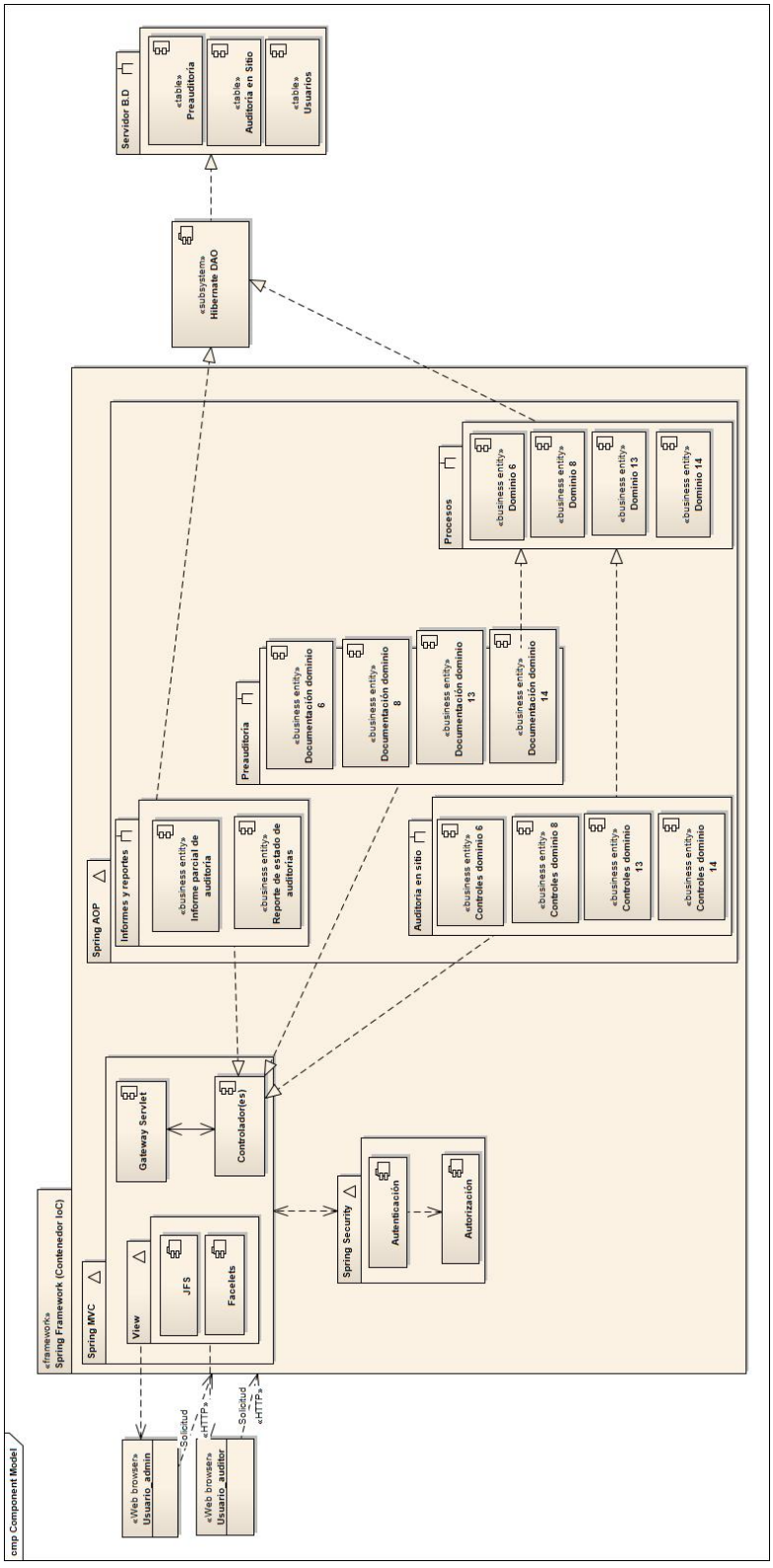
Cada capa está conformada por los siguientes componentes:

1. **Modelo:** Para permitir permitir el acceso a la información y base de datos asociadas, se propone un mecanismo de autenticación y autorización, el cual se instanciará desde la pantalla de inicio y asignación de roles correspondientes a cada tipo de usuario.

2. **Vista:** La vista de la arquitectura propuesta se basa en *JSF* (JavaServer Face, tecnología y framework de desarrollo para aplicaciones Java basadas en la Web, la cual simplifica

[1] Angel A., Miguel. Qué es MVC. [Online]: <*http://www.desarrolloweb.com/articulos/que-es-mvc.html*>

Figura 9.1: *Arquitectura del modelo auditoría en seguridad de la información para los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006*



Fuente: Autor

el desarrollo de interfaces de usuario) y *Facelets* (sistema de código abierto de plantillas Web bajo la Licencia Apache y tecnología de controlador de JSF).

3. **Controlador:** Se implementarán controladores para la comunicación de cada uno de los módulos de la arquitectura con la interfaz de usuario. Así mismo, se hará uso de *servlet* para ofrecer un contenido dinámico desde el servidor Web.

9.1.3. Spring Security

Spring Security proporciona servicios de seguridad para aplicaciones de software empresariales basados en J2EE, en proyectos desarrollados bajo Spring Framework. La seguridad de la aplicación comprenderá dos operaciones:

1. **Autenticación**, en el cual se establecen las reglas para establecer si el usuario que hará uso del aplicativo es quien dice ser.
2. **Autorización**, en el cual se determina las acciones permitidas en el aplicativo por el usuario autenticado.

9.1.4. Informes y reportes

Es módulo comprende las consultas correspondientes a los informes parciales de auditoría y los reportes de los estados de las auditorías realizadas o en proceso. Desde este módulo, el usuario podrá generar documentos en PDF para su impresión o como soporte de un proceso de auditoría ante una entidad certificadora o regulatoria.

9.1.5. Pre-auditoría

En este módulo se encuentran las herramientas de trabajo para realizar la pre-auditoría de los dominios 6, 8, 13 y 14 de acuerdo a lo establecido en las normas NTC-ISO 27001:2006 y NTC-ISO 27002:2007. Las herramientas se componen de las listas de chequeo para la revisión documental de cada uno de los dominios y los requisitos generales de un SGSI. Así mismo, contiene el formato para generar el plan de auditoría en sitio.

9.1.6. Auditoría en sitio

En este módulo se encuentran los papeles de de trabajo para la auditar cada uno de los controles de los dominios 6, 8, 13 y 14 del anexo A de la norma NTC-ISO/IEC 27001:2006, apoyados

en la norma NTC-ISO/IEC 27002:2007. Las herramientas alojadas en este módulo comprenden: Plan de auditoría (diligenciado en el modulo de Pre-auditoría), formato de reunión de apertura y lista de chequeo de controles.

9.1.7. Procesos

Este módulo comprende todo los procesos modelados en una herramienta de modelamiento de flujo de trabajo (como BizAgi o BonitaSoft). Cada proceso definirá la ruta de acción durante la ejecución de los dos momentos en una auditoría: pre-auditoría y auditoría en sitio.

9.1.8. DAO-Data Access Object

En este módulo se comprenden las reglas de negocio para el acceso a los repositorios del aplicativo, mediante una interfaz común entre la aplicación y los dispositivos de almacenamientos. Como herramienta de mapeo objeto-relacional (ORM por sus siglas en ingles), se propone el uso de *Hibernate*: un completo framework que permite agilizar la relación entre la aplicación y la base de datos.

9.1.9. Servidor BD

Este componente comprende el modelo de datos de la aplicación. Estará compuesto de tres bases de datos distintas, las cuales se relacionan con los módulos de pre-auditoría, auditoría en sitio y una para la administración de usuarios desde Spring Security.

9.2. Estructura de la arquitectura

La arquitectura propuesta, está diseñada en tres capas:

1. **Capa de presentación:** Conocida también como "capa de usuario" o "interfaz gráfica", tiene la función de mostrar, comunicar y capturar información de la aplicación al usuario de forma mas simple. Se compone de los módulos Spring MVC y Spring Security.
2. **Capa de aplicación:** Conocida también como "capa o lógica de negocio", aloja todos los programas a ejecutar para desarrollar las diferentes etapas de un proceso de auditoría. Es aquí donde se establecen todas las reglas que deben cumplirse para lograr un proceso

de auditoría eficiente. La componen los módulos Informes y reportes, Pre-auditoría, Auditoría en sitio y Procesos.

3. **Capa de datos:** Comprende el acceso y almacenaje de los datos de la aplicación. Está compuesta de los módulos DAO (Hibernate) y Servidor BD.

Del framework de Spring se hace uso de:

- **Contenedor IoC**, en las tres capas de la aplicación.
- **Spring Security**, en la capa de presentación.
- **Spring AOP**, para la capa de aplicación.

Para la capa de datos, sólo se hace uso de Hibernate como herramienta de mapeo.

RESULTADOS

En este apartado se presentan los resultados de los dos momentos del desarrollo del presente proyecto, con el fin de dar respuesta a la hipótesis planteada en el apartado *"Hipótesis y objetivos"*: la validación realizada por expertos del modelo general de auditoría propuesto y la ejecución de la prueba piloto en una empresa de la región.

10.1. VALIDACIÓN DE EXPERTOS

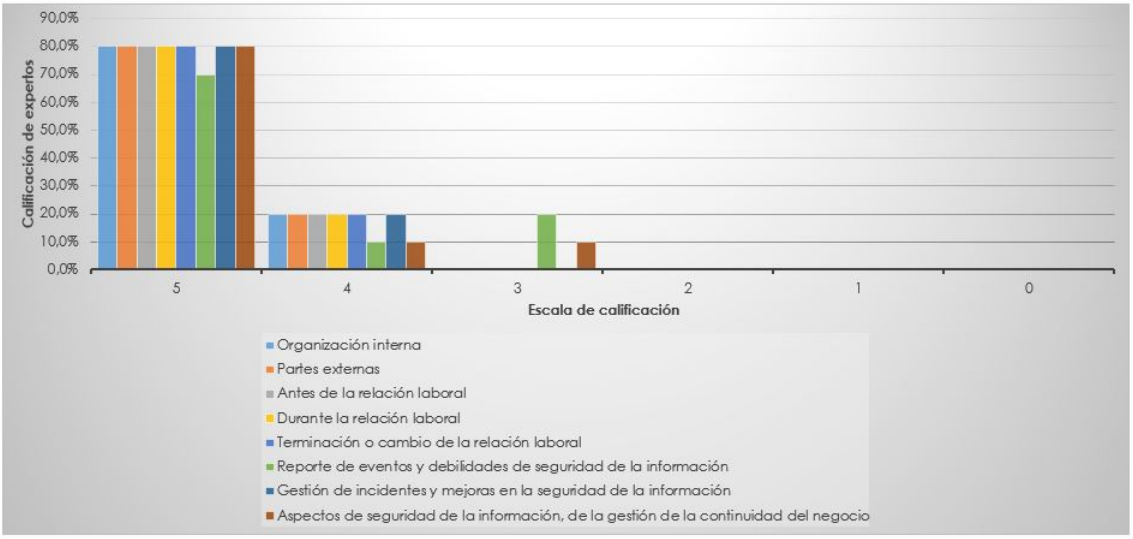
La validación se realiza mediante una presentación del modelo a un grupo de expertos. Se presentan todo los modelos y al final se realiza la evaluación por encuesta. La evaluación arroja los siguientes resultados:

1. En cuanto al cumplimiento del modelo respecto a la norma NTC-ISO/IEC 27001:2006:

   - Para los objetivos de control "Organización interna", "Partes externas", "Antes de la relación laboral", "Durante la relación laboral", "Terminación o cambio de la relación laboral" y "Gestión de incidentes y mejoras en la seguridad de la información", el 80 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, y el 20 % restante califica el modelo con un cuatro (4). No se presentan calificaciones de tres (3), dos (2), uno (1) o cero (0) puntos.
   - Para el objetivo de control "Reporte de eventos de seguridad de la información", el 70 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, un 10 % de ellos califican el modelo con un cuatro (4), y el 20 % restante califica el modelo con un tres (3). No se presentan calificaciones de dos (2), uno (1) o cero (0) puntos.
   - Para el objetivo de control "Aspectos de seguridad de la información, de la gestión de la continuidad del negocio", el 80 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, un 10 % de ellos califica con un cuatro (4) el modelo, y el 10 % restante califica con un tres (3). No se presentan calificaciones dos (2), uno (1) o cero (0).

   En el siguiente gráfico, se resume la validación realizada por parte de los expertos respecto al cumplimiento de la norma:

Figura 10.1: *Evaluación respecto al cumplimiento de la norma NTC-ISO/IEC 27001:2006*



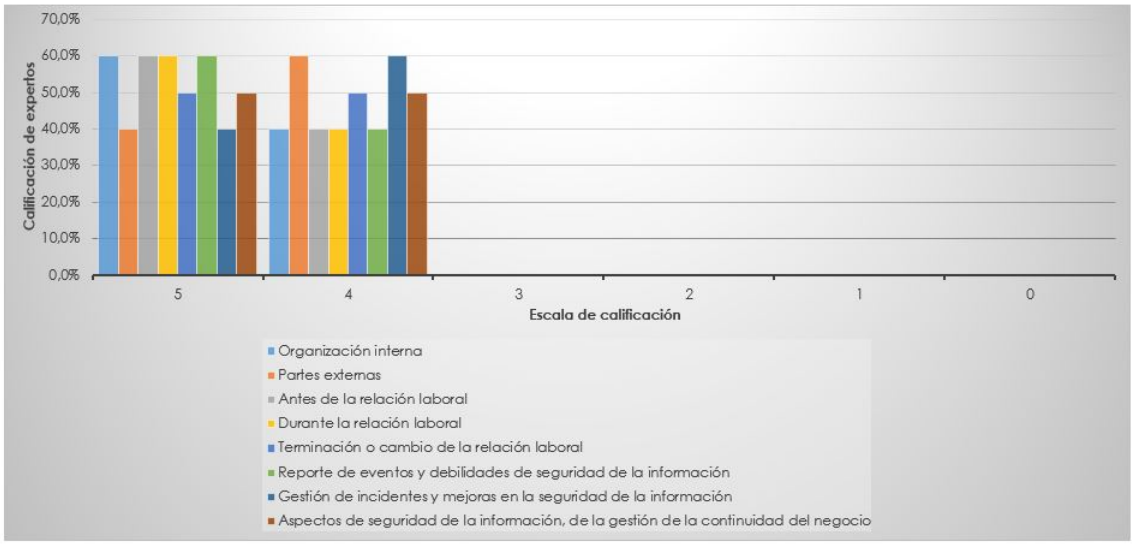
Fuente: Autor

2. En cuanto a la claridad del procedimiento de auditoría interna:

   - Para los objetivos de control "Organización interna", "Antes de la relación laboral", "Durante la relación laboral", "Reporte de eventos de seguridad de la información", el 60 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, y el 40 % restante califica el modelo con un cuatro (4). No se presentan calificaciones de tres (3), dos (2), uno (1) o cero (0) puntos.
   - Para el objetivo de control "Partes externas", "Gestión de incidentes y mejoras en la seguridad de la información", el 40 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, y el 60 % restante califican el modelo con un cuatro (4). No se presentan calificaciones de tres (3), dos (2), uno (1) o cero (0) puntos.
   - Para el objetivo de control "Terminación o cambio de la relación laboral", "Aspectos de seguridad de la información, de la gestión de la continuidad del negocio", el 50 % de los encuestados califican el modelo propuesto asociado a este objetivo de control con cinco (5) puntos, y el 50 % restante califican el modelo con un cuatro (4). No se presentan calificaciones tres (3), dos (2), uno (1) o cero (0).

   En el siguiente gráfico, se resume la validación realizada por parte de los expertos respecto a la claridad del procedimiento de auditoría:

Figura 10.2: *Evaluación respecto a la claridad del proceso de auditoría interna en seguridad de la información*



Fuente: Autor

La validación también permitió realimentar el proceso desarrollado durante el proyecto de grado. Esto permitió realizar mejoras en el modelo actual y plantear cambios posibles desde la perspectiva de los expertos. Las siguientes fueron la observaciones realizadas por los expertos:

- *Muy buen diseño de procesos, son coherentes y fáciles de interpretar.*
- *El modelado y los formatos desarrollados que se describen en el documento, suponen una base para que el auditor interno simplifique su tarea en el desarrollo de las actividades de auditoría; por lo tanto, en el formato empleado el campo "OBSERVACIONES" deben contener los documentos que permitan al auditor llevar a cabo la tarea de forma más eficaz.*
- *Los "PARTICIPANTES" suponen el personal de apoyo en la organización que estarán presentes cuando se realice la auditoría o a los cuales se les hará alguna consulta en caso de que surja una inquietud. Por ejemplo en el proceso principal "SEGURIDAD DE LOS RECURSOS HUMANOS" debe haber alguien del departamento de gestión humana que aparezca como participante en caso de querer realizar preguntas sobre los contratos, registros de evidencia frente a procesos disciplinarios llevados a cabo, etc.*
- *No se hacen evidentes en las actividades descritas, cuales de ellas se deben realizar en los diferentes momentos mencionados al comienzo (Previo - sitio).*
- *No obstante, y pese a las recomendaciones entregadas, las actividades descritas en el documento cumplen con los objetivos descritos en la norma ISO 27001:2005 y pueden ser implementadas como un modelo para realizar labores de auditoría.*

- *Revisar si la norma es ISO 27001:2005 o 2006.*
- *Para hacer una distinción entre los momentos de la auditoría y sus actividades, se podría estructurar de mejor manera los verbos, es decir, no usar en sitio "verificar" o "revisar" sino poner "corroborar", "Probar" o "realizar". Igual las actividades como están propuestas cumplen con el objetivo, pero se podría realizar una mejora dado que hay otro estudios similares.*
- *En el formato de auditoría en el campo "Observaciones" se menciona que deben estar disponibles los documentos de entrada y otros "documentos de soporte"; en este último seria bueno agregar cuales serian o cuales se deberían considerar.*

Las recomendaciones fueron tenidas en cuenta y ajustadas en el modelo antes de realizar la prueba piloto en la empresa de la región.

10.2. VALIDACIÓN DE MODELO MEDIANTE PRUEBA PILOTO

El objetivo de la prueba piloto era validar si el modelo de auditoría propuesto para los cuatro dominios de control objeto de estudio era aplicable en la práctica. La prueba piloto se lleva a cabo en una empresa de la ciudad de Pereira. La prueba solo contempla la etapa de pre-auditoría, cuyos resultados se muestran a continuación:

1. El modelo permitió establecer la documentación requerida para el proceso previo a la auditoría en sitio, tanto la información propia de un SGSI como la necesaria para validar cada uno de los dominios de control.
2. El modelo permitió definir rápidamente la ruta a seguir para realizar una adecuada revisión documental, documentación asociada a los objetivos de seguridad de la empresa.
3. Las herramientas resultantes, tanto para la pre-auditoría como para la auditoría en sitio, permiten desarrollar fácilmente el proceso y especificar los controles afectados al incumplir con el requisito exigido por la norma.
4. La herramienta de pre-auditoría permite generar un informe parcial más detallado y ordenado, según lo planteado por el modelo, así como identificar fácilmente no conformidades u observaciones en la estructura de seguridad actual planteado por la empresa.
5. La herramienta permitió definir oportunidades de mejora y establecer los puntos críticos de seguridad de la empresa. Desde este punto de vista, se encuentra que la empresa cumple con el 12 % de los requisitos exigidos por la norma en los dominios 6, 8, 13 y 14, equivalente a 6 requisitos de 51 a cumplir; el 88 % restante corresponde a incumplimiento,

encontrando 29 no conformidades, correspondientes a 13 no conformidades menores y 16 observaciones. También se encuentra que 16 requisitos no aplican para la empresa, por no contar con un control asociado implementado o no ser parte de sus objetivos de negocio.

El informe resultante, puede apreciarse con mayor detalle en el Apéndice C.

10.3. VALIDACIÓN DE LA HIPÓTESIS

A la pregunta: *"¿Es posible modelar un proceso de auditoría interna basado en procesos asociado a los dominios 6, 8, 13 y 14 del anexo A de la norma* ***NTC-ISO/IEC 27001:2006*** *que sirva de apoyo a los auditores internos para las auditorías de sistemas de información al momento de llevar a cabo una auditoría de seguridad de la información?"*, la respuesta es afirmativa. Como pudo apreciarse en la ejecución de los dos momentos del presente trabajo de grado, el modelado no solo permitió definir las actividades propias de una auditoría interna en seguridad de la información y establecer una ruta de trabajo adecuado para el auditor, sino también establecer los papeles de trabajo para los cuatro dominios objeto de estudio.

CONCLUSIONES

- Con el proyecto pudo demostrarse que es posible modelar procesos de auditoría interna en seguridad de la información mediante una herramienta de flujo de trabajo. Sin embargo, automatizar un proceso de auditoría interna haciendo uso de estas herramientas es limitante para algunas variables que se requieren sean flexibles o parametrizables, debido a la estructura misma de las herramientas de este tipo. Lo anterior se evidencia en trabajos anteriores realizados bajo la misma metodología[1][2].

- Modelar los procesos de auditoría asociados a los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006 permitió una mejor compresión de las actividades asociadas a cada subproceso generado, no solo por la ruda que debe seguirse para ejecutar un proceso dado, sino por justificar la razón por la cual debe realizarse determinada tarea antes de continuar la siguiente.

- El estudio realizado para identificar las actividades a realizar para validar los controles asociados a los dominios 6, 8, 13 y 14 de la norma NTC-ISO/IEC 27001:2006 permitió generar herramientas genéricas para cualquier auditoría interna en seguridad de la información donde se incluyan estos, como identificar aquellos requisitos que son comunes para un grupo de controles.

- Una actividad clave para contar con un modelo de auditoría coherente, completo y aplicable fue realizar la validación por parte de expertos en tema de seguridad de la información. Los aportes resultantes de la presentación del modelo permitió ajustarlo de acuerdo al estándar tomado como base; así mismo, sus observaciones permitieron llevar a cabo la prueba piloto con mayor seguridad y ejecutarla siguiendo las pautas establecidas por la norma.

- El modelado permitió definir una propuesta de arquitectura para automatizar las herramientas y los modelos de auditoría, la cual estaría orientada a la Web; para ello se propone una arquitectura basada en Spring Framework, Java (como lenguaje de programación) e Hibernate. Es necesario automatizar el proceso de auditoría para contar con una herramienta útil dirigida a los auditores internos en seguridad de la información, que permite la generación automática de reportes e informes de auditoría. La prueba piloto realizada en la empresa de la región, contó con el componente tecnológico, pero la mayoría de las actividades fueron realizadas de manera manual, lo cual evidenció la falta de una herramienta automatizada para desarrollar el proceso de más eficientemente.

- Con el proyecto fue posible validar la hipótesis planteada, obteniendo una respuesta

[1]Paula A. Villa S. DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TICS. Universidad Tecnológica de Pereira, 2011.

[2]Edward F. Penagos G. MÓDULO DE GESTIÓN DE AUDITORÍA SOPORTADO EN TIC PARA LA GESTIÓN DE COMUNICACIONES, SEGUIMIENTO Y REVISIÓN DEL SGSI. Universidad Tecnológica de Pereira, 2014

afirmativa. En la practica, tanto la validación dada por los expertos como en la ejecución de la prueba piloto en la empresa de la región, los resultados fueron los esperados.

- Con la prueba piloto pudo evidenciarse la ventaja de contar con una herramienta que permita identificar vulnerabilidad de seguridad y oportunidades de mejora para la empresa auditada. También fue clara la utilidad de aplicación del modelo en organizaciones que no cuentan con un SGSI implementado; aún con aplicación de buenas prácticas de seguridad se muestran brechas que pueden subsanarse con las medidas adecuadas una vez éstas son identificadas. Lo anterior demuestra que el modelo puede ser aplicado en cualquier tipo de organización, sin importar o no la aplicación de buenas prácticas en seguridad de la información en sus procesos de negocio.
- El proyecto tardó más de lo esperado debido a la participación del autor en otros proyectos relacionados, permitiendo la retroalimentación y aumentar la base de conocimiento, no solo del presente proyecto de grado sino de aquellos en los cuales se toma parte, pero sin dejar de lado el desarrollo del mismo. De esta manera se permitió brindar bases para un proyecto ejecutado en la ciudad de Pereira en una empresa de carácter mixto en el tema de seguridad de la información, y establecer la ruta de trabajo para proyectos actualmente desarrollados por la universidad en la misma temática.

RECOMENDACIONES

- Para modelar un proceso de auditoría asociado a la seguridad de la información, o de cualquier otro tipo, el hacer uso de una herramienta de flujo de trabajo como BizAgi o BonitaSoft es una buena elección, no solo por la presentación sino por los estándares de BPMN en el cual fueron diseñados estas plataformas. Sin embargo, al momento de automatizar estos procesos modelados, lo recomendable es hacer uso de framewoks de desarrollo y elegir un lenguaje de programación adecuado y flexible para realizar la automatización desde cero. Estas herramientas de flujo de trabajo en la práctica han demostrado ser muy limitadas para automatizar procesos de este tipo.

- Si se desea automatizar un proceso en una herramienta de flujo de trabajo, lo ideal es trabajar con la versión mas reciente del aplicativo. Durante el desarrollo del proyecto se generaron reprocesos debido a la incompatibilidad de las versiones de cada herramienta, lo cual provocaba, en la mayoría de la veces, iniciar el proceso de modelado desde cero. Así mismo, deben desarrollar los modelos en una misma herramienta, ya que no todas las casas desarrolladoras manejan un estándar BPMN que sea compatible entre ellas.

- Como se mencionó anteriormente, la mejor alternativa para automatizar procesos de auditoría es realizando la aplicación desde cero, apoyados en un framework de desarrollo y un lenguaje de programación flexible. Desde este punto de vista, proyectos automatizados anteriormente bajo herramientas de flujo de trabajo deben ser analizados nuevamente y automatizarlos a partir de una arquitectura de software definida.

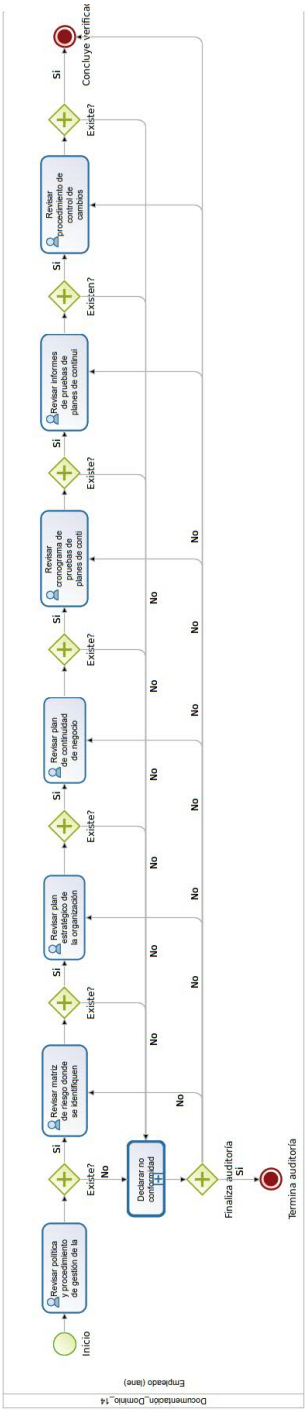
- Debido a la actualización de la norma NTC-ISO/IEC 27001 en su versión 2013, es necesario ajustar los modelos desarrollados en este proyecto de grado y los demás realizados bajo la norma en sus versiones 2005 y 2006, para contar con un modelo general de auditoría de seguridad de la información acorde a la normatividad vigente, y sirva de herramienta para los auditores internos en seguridad de la información.

Parte I

APÉNDICES

Apéndice DOMINIO 14 PREVIO

Figura A.1: *Aspecto "Gestión de la continuidad del negocio".*



Fuente: Autor

Apéndice HERRAMIENTAS PARA EL PROCESO DE AUDITORÍA INTERNA

Apéndice INFORME PARCIAL DE PRE-AUDITORÍA

Bibliografía

[1] Benavides B., Herney N. and Ortiz G., Leandro J. *IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA UN SISTEMA DE GESTIÓN Y MONITOREO DE EVENTOS DE SEGURIDAD EN LA RED DE DATOS DE LA UNIVERSIDAD TECNOLÓGICA DE PEREIRA*. Universidad Tecnológica de Pereira, 2011.

[2] Sierra J., Oscar Andrés. *ESTUDIO DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN DIGITAL EN LAS EMPRESAS DEL DEPARTAMENTO DE RISARALDA*. Universidad Tecnológica de Pereira, 2011.

[3] Villa S., Paula A. *DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TIC'S*. Universidad Tecnológica de Pereira, 2011.

[4] Penagos G., Edward F. *Módulo de Gestión de Auditoría Soportado en TIC para la Gestión de comunicaciones, seguimiento y revisión del SGSI*. Universidad Tecnológica de Pereira, 2014.

[5] Dey, Manik. *INFORMATION SECURITY MANAGEMENT - A PRACTICAL APPROACH*. IEEE Computer Society, 2010.

[6] Hensel, Veselina and Lemke-Rust, Kerstin. *ON AN INTEGRATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM INTO AN ENTERPRISE ARCHITECTURE. 2010 Workshops on Database and Expert Systems Applications*. IEEE Computer Society, 2010.

[7] Mana G., Joel. *PRIVACY AND INFORMATION SECURITY IN BRAZIL? YES, WE HAVE IT AND WE DO IT!. 2010 Seventh International Conference on Information Technology*. EEE Computer Society, 2010.

[8] Milicevic, Danijel and Goeken, Matthias. *APPLICATION OF MODELS IN INFORMATION SECURITY MANAGEMENT.*. IEEE Computer Society, 2011.

[9] Villa S., Paula A.. *DEFINICIÓN DE PROCESOS DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SOPORTADO EN TIC'S.*. IEEE Computer Society, 2011.

[10] Montesino, Raydel and Fenz, Stefan.. *AUTOMATION POSSIBILITIES IN INFORMATION SECURITY MANAGEMENT. 2011 European Intelligence and Security Informatics Conference.*. IEEE Computer Society, 2011.

[11] Díaz P., Flor N.. *Principales estándares para la seguridad de la información IT. Alcances y consideraciones esenciales de los estándares*. Eos. Volumen 2, 2008.

[12] Cano, Jeimy. *III Encuesta Latinoamericana de Seguridad de la Información ACIS 2011.* [Online]: *http://www.acis.org.co/fileadmin/Base_ de_ Conocimiento/XI_ JornadaSeguridad/Presentacion_ Jeimy_ Cano_ III_ ELSI.pdf.* ACIS, 2011.

[13] Almanza, Andrés. *IX Encuesta Nacional de Seguridad Informática en Colombia.* [Online]: *http://www.acis.org.co/fileadmin/Base$_d$e$_C$onocimiento/XI_JornadaSeguridad/−Presentacion_Andres_Almanza_XI_JNSI.pdf.ASIC*, 2012.

[14] *VI Encuesta Latinoamericana de Seguridad de la Información ACIS 2014.* [Online]: *http://www.acis.org.co/fileadmin/Base_ de_ Conocimiento/XIV_ JornadaSeguridad/ELSI_ 2014.pdf.* ASIC, 2014.

[15] Lerma, Héctor D. *Metodología de la Investigación: Propuesta, Anteproyecto y Proyecto.* , 20.

[16] *Estándar Internacional ISO/IEC 17799. Tecnología de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información.* ISO. Segunda edición, 2005.

[17] *Sistema de gestión de la calidad. Conceptos y vocabulario. Norma NTC-ISO 9000.* ICONTEC, 2005.

[18] *Código de buenas prácticas para la gestión de Seguridad de la Información. Norma NTC-ISO/IEC 27002.* ICONTEC, 2007.

[19] *Compendio Tesis y otros trabajos de grado, con la reforma a la norma NTC-ISO 1486.* ICONTEC, 2007.

[20] *Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos. Norma NTC-ISO/IEC 27001.* ICONTEC, 2006.

[21] *Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos. Norma NTC-ISO/IEC 27001.* ICONTEC, 2013.

[22] *COBIT 4.1. Marco de trabajo - Objetivos de control - Directrices gerenciales - Modelo de madurez.* IT Governance Institute, 2007.

[23] *Alineando COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa. Un reporte para gestión del ITGI y la OGC.* [Online]: *http://www.ISACA.com/.* IT Governance Institute, 2011.

[24] *Cobit 5 y la Seguridad de la información.* [Online]: *http://www.ISACA.com/.* IT Governance Institute, 2011.

[25] Blanco D., Jorge A. *Auditoría de sistemas.* Escuela superior de administración pública.

[26] Durán J., Miguel A. *Metodología de una auditoria de sistemas.* [Online]: *http://www.itchetumal.edu.mx/paginasvar/Maestros/mduran/Archivos/METODOLOGIA %20DE %20UNA %20AUDITORIA %20DE %20SISTEMAS.pdf.* Instituto Tecnológico de Chetumal.

[27] *Bizagi, Centro de documentación*. [Online]: *http://wiki.bizagi.com/es/index.php?title=-Main_ Page*. Bizagi.

[28] *BizAgi BPM Suit*. [Online]: *http://www.bizagi.com*. Bizagi.

[29] *ISO 27000.es*. [Online]: **www.iso27000.es**.

[30] *Más de 1900 millones de pesos en multas por infracciones a la ley 1266*. [Online]: *http://habeasdatacolombia.uniandes.edu.co/?p=168*. Universidad de los Andes, 2011.

[31] *41 personas condenadas por el delito de violación de datos personales y 544 multas por infracción de la ley 1266 de 2008*. [Online]: *http://habeasdatacolombia.uniandes.edu.co/?p=980*. Universidad de los Andes, 2013.

[32] *Bonita BPM 6.4*. [Online]: *http://es.bonitasoft.com/*. Bonitasoft.

[33] *BonitaSoft BPM*. [Online]: *http://intellego.com.mx/en/node/636*. Intellego.

[34] *Bonita open solution - Evento de Gobierno 2013*. [Online]: *http://www.slideshare.net/grupointellego/bonita-open-solution-18630096*. Intellego, 2013.

[35] Canales M., Roberto. *Primeros pasos con Bonita BPM Community 6.2.6*. [Online]: *http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=bonita_ bpm_ primeros_ pasos*. 2014.

[36] *Introducción a Spring Framework*. [Online]: *https://jaehoo.wordpress.com/2010/11/28/introduccion-a-spring-framework/*. 2010.

[37] Gavidia, Carlos G. *Arquitectura y diseño de aplicaciones JAVA EE*. [Online]: *http://www.slideshare.net/cptanalatriste/arquitectura-y-diseo-de-aplicaciones-java-ee?from=ss/_ embed*. Avances Tecnológicos SGL.

[38] Márquez S., Santiago. *Introducción a Spring Segurity*. [Online]: *http://es.slideshare.net/SantiagoSolis1/spring-security-6890070*.

[39] Reyes Z., José J.. *2da. reunión Java Querétano. Introducción a Spring Framework*. [Online]: *http://es.slideshare.net/neodevelop/spring-presentation*. SynergyJ.

[40] Johnson, Rod and *others*. *Spring Framework Reference Documentation*. [Online]: *http://docs.spring.io/spring/docs/4.1.0.RC2/spring-framework-reference/htmlsingle/*. 2014.

Lista de acrónimos

ACIS: *Colombiana de Ingeniería de Sistemas*
BD: *Base de datos*
BPMN: *Business Process Model and Notation - Modelo y Notación de Procesos de Negocio*
BU: *Bussines Unit - Unidades de negocio*
DAO: *Data Access Object - Objeto de Acceso a Datos*
IEC: *International Electrotechnical Commission*
BD: *Inversion of Control - Inversión de control*
ISO: *International Organization for Standardization*
ORM: *Object-Relational Mapping - Mapeo Objeto-Relacional*
NTC: *Norma Técnica Colombiana*
SGSI: *Sistema de Gestión de Seguridad de la Información*
ITC: *Tecnología de la Información y la Comunicación*